UNIVERSIDAD PABLO DE OLAVIDE

FACULTAD DE DERECHO

TESIS DOCTORAL:

"LA CONTRATACIÓN DEL *CLOUD COMPUTING*"

Presentada por ÁNGEL MANUEL DOMÍNGUEZ GARCÍA para la obtención del título de Doctor en Ciencias Jurídicas y Políticas por la Universidad Pablo de Olavide de Sevilla.

DIRIGIDA POR:

PROF. DR. AGUSTÍN MADRID PARRA

Depositada en Sevilla, a 05 de octubre de 2018

A mis padres,

sin ellos no hubiera sido posible.

A Lola,

ella ha vivido el proceso conmigo.

A la educación pública,

uno de tus hijos.

RESUMEN

Las comunicaciones electrónicas han sufrido un proceso revolucionario con la aparición de Internet, como herramienta universal y global, capaz de canalizar las relaciones entre personas, empresas y Administraciones.

La virtualización y el intercambio de datos requiere de un proceso de ingeniería que permita a las personas, físicas y jurídicas, analizar la información producida, con el objetivo de mejorar los procesos y su ventaja competitiva.

Los dispositivos electrónicos actuales han adoptado el *cloud computing* como configuración básica para el correcto desempeño de sus objetivos. La flexibilidad, la rápida adaptación, conectividad y costos asociados son las características básicas de la herramienta que han acuciado el empleo de la tecnología de la nube.

La aparición de los contratos informáticos y electrónicos supuso un replanteamiento de las estructuras jurídicas en materia de contratos. Sobre la base de ese estudio doctrinal, esta nueva realidad en las transacciones económicas debe ser tratada, teniendo presente siempre los problemas nacientes ante la utilización del *cloud computing*.

El contrato se erige como instrumento jurídico que regulará el devenir del servicio, siendo el objetivo del presente trabajo un estudio holístico de la contratación en la nube que nos permita vislumbrar los derechos y obligaciones cuando empleamos la herramienta electrónica, aproximándonos al marco jurídico aplicable, armonizado con una visión eminentemente práctica. Los clientes, rara vez, analizan los términos y condiciones que regularán el uso de la nube, impuestos por los proveedores. Conocer el clausulado común de la nube permitirá un consentimiento informado del cliente y comprender las consecuencias jurídicas de la adopción de las disposiciones, los modos de protección y las responsabilidades de las partes en caso de incumplimiento.

ÍNDICE

ACRÓNIMOS Y ABREVIATURAS 10

INTRODUCCIÓN 15

CAPÍTULO I – DELIMITACIÓN DEL *CLOUD COMPUTING* 19
- **a. Definición y características** 20
- **b. Potenciales riesgos de la adopción del *cloud computing*** 28

CAPÍTULO II – CONTRATOS INFORMÁTICOS Y POR MEDIOS ELECTRÓNICOS 37
- **a. Qué son los contratos informáticos y los contratos por medios electrónicos** 38
- **b. Los bienes informáticos: definición** 42
- **c. La regulación actual de los contratos electrónicos** 43
- **d. Principios comunes y específicos en el marco del comercio electrónico** 49
- **e. En relación con el contrato del *cloud computing*** 59

CAPÍTULO III – INICIATIVAS LEGALES 63
- **a. Anteproyecto de Ley de Código Mercantil Español** 64
  - *a. Introducción. Principios comunes y específicos en el marco del comercio electrónico* 64
  - *b. Tipificación de los contratos de comunicaciones electrónicas* 68
    - *i. Contrato de servicios de comunicación electrónica* 69
    - *ii. Contrato de alojamiento de datos* 76
    - *iii. Acuerdos para la copia temporal de datos o información* 78
  - *c. Incidencia del Anteproyecto de Ley de Código Mercantil en la contratación del cloud computing* 79
- **b. Actividad del Grupo Europeo de Protección de Datos "artículo 29"** 83
  - *a. Introducción: qué es el Grupo de Trabajo del artículo 29 y contexto en la prestación del servicio del cloud computing* 83
  - *b. Recomendaciones del Grupo de Trabajo del artículo 29 para la prestación del servicio del cloud computing* 85
- **c. Experiencias internacionales** 95
  - *a. Primeros pasos: FedRAMP de EEUU* 97
  - *b. UK Government G-Cloud, una propuesta de Acuerdos Marcos para la computación en la nube en la Administración pública de Reino Unido.* 102
  - *c. Canada Right Cloud, la adopción de la nube solo cuando es necesario* 107
  - *d. Grupo de Trabajo IV (Comercio Electrónico) de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional* 110
  - *e. Conclusiones* 121

CAPÍTULO IV – DISPOSICIONES REGULATORIAS, SU INCIDENCIA EN EL CONTENIDO DEL CONTRATO 124
a. El contrato para garantizar la seguridad, la protección y el equilibrio en el *cloud computing* 125
b. Cliente y proveedor en el contrato de la nube a luz de la normativa protectora de datos de carácter personal 131
a. Acceso a los datos por el prestador de servicios en la nube 137
b. Subcontratación en la prestación de servicios de cloud computing 150
c. Transferencia internacional de datos personales 156
d. Proyecto de Ley Orgánica de Protección de Datos de carácter Personal 169

CAPÍTULO V – EL CONTRATO DE *CLOUD COMPUTING* 173
a. La prestación de servicios del *cloud computing* entre empresas 175
a. Condiciones generales en el contrato del cloud computing 183
i. Contratantes, parte expositiva y el objeto del contrato 184
ii. Obligaciones de las partes 187
iii. Protección de datos de carácter personal 190
iv. Duración y terminación del contrato 193
v. Jurisdicción y ley aplicable 196
b. Cláusulas específicas en el contrato de cloud computing 199
i. Responsabilidad 201
ii. Uso aceptable 207
iii. Localización y tratamiento de los datos 210
iv. Seguridad en el servicio 215
v. Lock-in y lock-out 221
vi. Derechos de Propiedad Intelectual e Industrial 225
vii. Acuerdo de Nivel de Servicios (ANS o SLA) 228
viii. Cambio de las características del servicio y renovación del ANS 234
c. Epítome sobre la extinción del contrato de computación en la nube entre empresas: causas y efectos de las obligaciones 236
b. La protección del consumidor en el contrato de *cloud computing* 242
a. Definición de consumidor a la luz de la normativa aplicable 245
i. Consumo mixto 249
b. Cláusulas generales de contratación, cláusulas no negociadas individualmente y cláusulas de protección al consumidor 252
c. Análisis de las cláusulas contractuales en la prestación del cloud cuando el cliente es un consumidor 261
i. Protección al consumidor de la nube antes de la perfección del contrato 261
ii. Ámbito de aplicación 266
iii. Protección ex post, estudio de las cláusulas contractuales en la contratación con consumidores 269
a. Protección de datos 269
b. Variación de los términos del contrato 272
c. Jurisdicción y sumisión al arbitraje 275
d. Ley aplicable 279
e. Responsabilidad 282

f. Uso aceptable 286
g. Localización y tratamiento de datos 288
h. Garantías y devolución del crédito por servicios no consumidos 290
i. Acuerdo de Nivel de Servicios (ANS o SLA), cambios y renovación 292
j. Extinción del contrato 294
c. La contratación del *cloud computing* en el sector público 296
a. El empleo de los medios electrónicos en las Administraciones públicas. Mimbres para la utilización de la nube 296
b. Tipo contractual del cloud computing según la normativa administrativa 310
c. Cláusulas necesarias en el contrato administrativo 315
d. Experiencias de la contratación del cloud computing en el sector público y breves notas sobre la Red SARA 324
i. La nube para PATRIMONIO NACIONAL 325
ii. La nube para RED.es 329
iii. La red SARA para las Administraciones públicas en España 336

CONCLUSIONES 338

BIBLIOGRAFÍA 349

RECURSOS ELECTRÓNICOS ANALIZADOS 369

JURISPRUDENCIA 375

ACRÓNIMOS Y ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
ANS o SLA	Acuerdo de Niveles de Servicios o Service Level Agreement
API	Interfaz de Programación de Aplicaciones
ATO	Autorización de funcionamiento en FedRAMP
AUP	Acceptable Use Policy o Política de Usos Aceptables
B2B	Business-to-business
BCR o NCV	Binding Corporate Rules o Normas Corporativas Vinculantes
C-SIG	Cloud Select Industry Group
CC	Código Civil - Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil
CCo	Código de Comercio - Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio
CCS	Crown Commercial Service (G-Cloud)
CLOUD Act	Clarifying Lawful Overseas Use of Data Act, EE.UU.
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
CORA	Comisión para la Reforma de las Administraciones Públicas, España
CPU	Unidad de Procesamiento Central
CVSS	Common Vulnerability Scoring System
DCE	Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)
DEUC	Documento Europeo Único de Contratación
DHS	United States Department of Homeland Security – Departamento de Seguridad Interna (Seguridad Nacional), EE.UU.
DOUE	Diario Oficial de la Unión Europea

DOD	United States Department of Defense – Departamento de Defensa, EE.UU.
DPD	Delegado de Protección de Datos
EEE	Espacio Económico Europeo
EE.UU.	Estados Unidos de América
eIDAS	Electronic Identification and Signature, referente al Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
ENISA	European Network and Information Security Agency o Agencia Europea de Seguridad de las Redes y de la Información
ENI	Real Decreto 4/2010, de 8 de enero, que aprueba el Esquema Nacional de Interoperabilidad
ENS	Real Decreto 3/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation, EE.UU.
FedRAMP	Federal Risk and Authorization Management Program, EE.UU.
FISMA	The Federal Information Security Management Act of 2002 – Ley Federal de Seguridad de Información, EE.UU.
G-Cloud	UK Government G-Cloud
GSA	U.S. General Services Administration – Administración de Servicios Generales, EE.UU.
GT 29	Grupo Europeo de Protección de Datos del artículo 29
IaaS	Infrastructure as a Sevice o Infraestructura como un Servicio
IDS	Sistema de Detección de Intrusiones
INCIBE	Instituto Nacional de Ciberseguridad, España
INTECO	Instituto Nacional de Tecnologías de la Comunicación, actualmente INCIBE, España
IoT	Internet of Things o Internet de las Cosas

IPS	Sistema de Prevención de Intrusos
ISO	Organización Internacional de Normalización o International Organization for Standardization
IT	Information Technology o Tecnología de la Información
JAB	Junta de Autorización Conjunta o Junta Mixta de Autorización del FedRAMP
LAE	Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos
LCD	Ley 3/1991, de 10 de enero, de Competencia Desleal
LCGC	Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación
LCME	Ley Modelo de la CNUDMI sobre Comercio Electrónico, 1996
LCSP	Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014
LSSICE	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LPACAP	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
LRJSP	Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
MMC	Medios Masivos de Comunicación
NIST	National Institute of Standards and Technology, EE.UU.
NSA	National Security Agency, EE.UU.
NCV o BCR	Normas Corporativas Vinculantes o Binding Corporate Rules
OBSAE	Observatorio de Administración Electrónica
OMB	Office of Management and Budget, USA - Oficina de Administración y Presupuesto, EE.UU.
OMPI	Organización Mundial de la Propiedad Intelectual

ONTSI	Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, España.
P2P	Red de pares, red entre iguales o red entre pares
P-ATO	Autorización provisional para operar en FedRAMP
PaaS	Platform as a Service o Plataforma como Servicio
PLOPD	Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, España
PMO	Oficina de Gestión de Proyectos de FedRAMP
PYMES	Pequeñas y medianas empresas
QoS	Niveles de Calidad
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
SaaS	Software as a Service o Software como Servicio
SCS	Cloud Services Specialist
SEPD	Supervisor Europeo de Protección de Datos
SLA o ANS	Service Level Agreement o Acuerdo de Niveles de Servicio
SLI	Niveles de indicación del servicio
TRLCSP	Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público
TRLCU	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios
UE	Unión Europea
USA	Estados Unidos de América

INTRODUCCIÓN

Internet se ha convertido en una herramienta universal y global para las comunicaciones, las transacciones económicas y, en general, la virtualización de las relaciones entre personas, empresas y Administraciones. Desde que despertamos estamos conectados a diferentes dispositivos móviles. En nuestro trabajo, hacemos uso de las herramientas electrónicas en búsqueda de una mayor eficiencia y conectividad. Nuestras relaciones con las Administraciones públicas tienden a ser plenamente virtuales. La sociedad está cada vez más instrumentalizada. Las personas, físicas y jurídicas, lejos de hacinar los datos y la información producida, propia o de terceros, utiliza la ingeniería para mejorar sus procesos y su ventaja competitiva. Esta capacidad de estructurar datos abre un amplio abanico de posibilidades para usuarios, empresas e Instituciones públicas.

La computación en la nube ha supuesto una revolución en el sector de las TIC por la flexibilidad, rápida adaptación, conectividad y costos asociados. La prosopopeya atribuida al *cloud*, como compañero en nuestros quehaceres diarios, ha acuciado su empleo. La nube proporciona a los usuarios una capacidad casi ilimitada de recursos y completamente accesibles, si bien, esta evolución está coligada con problemas de seguridad, disponibilidad o privacidad.

Los *smartphones*, los *wearables*, las aplicaciones ofimáticas, las ventanas electrónicas de la administración, las campañas de marketing, las *smart homes* e incluso las *smart cities*, por citar algunos ejemplos, adscriben la computación en la nube en su configuración para el correcto desempeño de las funciones objetivos. Este desarrollo tecnológico conmina a los ciudadanos, las empresas y las Administraciones al empleo del *cloud*, incluso aunque rehúsen del estar “siempre conectados”.

El citado empoderamiento que producen las herramientas informáticas, entre ellas el *cloud computing,* no es más que una añagaza, por cuanto el mercado se ha copado de grandes proveedores que han alcanzado un volumen de negocio y un grado de poder de control por la ingente información y datos que le suministramos. Esto propicia relaciones asimétricas entre clientes y prestadores, afectando a la seguridad, confidencialidad y equilibrio del servicio.

El advenimiento de la computación en la nube requiere respuestas de índole jurídico. El carácter supranacional e, incluso, a veces ignoto de la herramienta, dificultan regular normativamente la materia, propiciando la autorregulación entre partes.

El contrato se erige como instrumento jurídico que regulará el devenir del servicio, siendo el objetivo del presente trabajo un estudio holístico de la contratación en la nube que nos permita vislumbrar los derechos y obligaciones cuando empleamos la herramienta electrónica, aproximándonos al marco jurídico aplicable, armonizado con una visión eminentemente práctica. Esta labor se traducirá, por tanto, en un análisis conjunto de la normativa aplicable y las cláusulas dispuestas por los principales proveedores del servicio.

Delimitar qué es el *cloud computing* es nuestro punto de partida. Conocer las características esenciales, siempre empleando una concepción neutra que no merme la evolución de la tecnología, sus modelos de implantación y los diferentes modelos o clases del servicio, serán el punto de partida para delimitar el objeto y, por ende, las obligaciones principales a cumplir por el prestador del servicio.

Seguidamente, debemos hacernos acopio del acervo jurídico de los contratos informáticos, que por razón del objeto comparten características con el *cloud*, así como de la extensa regulación en función del medio por el cual se produce la contratación, que condicionará el marco regulatorio del servicio. Ante un mercado relativamente inmaduro, los principios comunes y específicos del comercio electrónico, reconocidos, al menos en parte, en normas sectoriales, permitirán adaptar las disposiciones jurídicas a la realidad, a la práctica. No solo para la validez jurídica en la contratación del servicio, sino para el proceso y desarrollo de la herramienta, principalmente cuando se emplea en el seno de las Administraciones públicas y, por tanto, bajo el régimen administrativo.

Conocer las iniciativas legales, nacionales e internacionales, además de permitirnos reflexionar sobre la perspectiva adoptada desde los diferentes entes que han debatido, de forma global o temática, sobre la regulación de la nube, centrará el objeto de estudio, al conocer los problemas comunes a los que se enfrentan los sujetos contratantes, independientemente de la naturaleza jurídica. De igual modo, estas propuestas han marcado la presentación de ofertas de la nube, por lo tanto, aunque sea de manera indirecta, repercutirá en el análisis de la contratación. En este enfoque, tiene un papel prioritario el estudio del Anteproyecto de Ley de Código Mercantil Español, porque, a

pesar de su olvido, ha supuesto plasmar de forma expresa los principios comunes del comercio electrónico de forma global y, porque de forma particularizada, reconoce la idiosincrasia de los contratos de comunicaciones electrónicas, estableciendo un régimen de obligaciones acorde con las especificaciones y características de los contratos. Igualmente, el Grupo de Trabajo del artículo 29 ha hecho una labor encomiable en los estadios embrionarios de la nube. Fruto de toda esa ingente tarea es el reconocimiento en el RGPD, aunque no de forma expresa, de un régimen propicio para esta evolución tecnológica.

Con estas mimbres, se analizará el clausulado estandarizado de los contratos de computación en la nube, que, combinando el vacío normativo y la posición dominante en el mercado de los grandes proveedores, tienden a imponer cláusulas favorables, frecuentemente desproporcionadas, a los intereses de los prestadores. El objetivo principal ha sido conocer la práctica habitual de los proveedores, establecer los diferentes medios de protección y, en última instancia, dotar al lector de los conocimientos adecuados para un consentimiento informado y medios para una correcta protección. En este marco intentaremos analizar el alcance de la nube, los niveles de servicio y disponibilidad de los proveedores, las obligaciones en materia de seguridad y protección de datos, la localización de los *data centers*, las responsabilidades de las partes y las obligaciones y derechos que subsisten extinto o resuelto el contrato. Partiendo del marco general de una relación entre empresas, las singularidades en la contratación con consumidores y, por otra parte, la actuación de las Administraciones públicas como órganos de contratación, ante un excelso control, obligan a analizar las implicaciones jurídicas desde diferentes ópticas. Por consiguiente, se disecciona la estructura y diseño de la contratación de la nube en las relaciones entre empresas, cuando contrata un consumidor o usuario y cuando las Instituciones públicas son parte activa del proceso.

Antes de centrarnos en el contrato de *cloud computing*, hemos considerado oportuno establecer las obligaciones y responsabilidades del cliente y proveedor de la nube para la garantía de la protección de datos de carácter personal. Las diferentes iniciativas internacionales se centran en la regulación de la seguridad e integridad de los datos en el servicio, principalmente aquellos con conexión internacional. Más cuando, por razón de ser, contratan el servicio entes del sector público que, a la ingente cantidad de datos, se une la naturaleza de los mismos y las implicaciones de sus procesos y expedientes en los administrados. La mecánica del *cloud computing* favorece que los datos y ficheros de los

diferentes agentes que contraten el servicio se encuentren ubicados fuera de las fronteras nacionales, dificultando el cumplimiento de la normativa de protección de datos en España. Con la vigencia del RGPD, el elenco de obligaciones de los responsables y encargados del tratamiento de datos y el endurecimiento de las sanciones en caso de incumplimiento, requieren de un conocimiento exacto de las actividades permitidas por los clientes, así como del deber de diligencia en sus actuaciones. Por lo tanto, el estudio de las cláusulas contractuales que regirán las obligaciones de las partes del contrato debe combinarse con el régimen protector de los datos personales, intentando compatibilizar la libre circulación de datos con una protección adecuada del derecho fundamental.

Esta tesis tiene como germen el trabajo realizado en el Máster Universitario de Derecho de las Nuevas Tecnologías de la Universidad Pablo de Olavide de Sevilla. En aquella ocasión, y en esta, no hubiera sido posible su elaboración y conformación sin la ayuda, colaboración y corrección del Prof. Dr. Agustín Madrid Parra.

Capítulo I - DELIMITACIÓN DEL *CLOUD COMPUTING*. a. Definición y características. b. Potenciales riesgos de la adopción del *cloud computing*.

CAPÍTULO I – DELIMITACIÓN DEL *CLOUD COMPUTING*

a. Definición y características

No existe un concepto generalizado de computación en la nube o *cloud computing*. Quienes se aventuran a definir el servicio vienen a hacer referencia a las características que actualmente incorpora el recurso, más que a la propia concepción del mismo.

La Comisión Europea parte de una definición simple para indicar que *"la computación en la nube consiste en el almacenamiento de datos (tales como archivos de texto, imágenes y video) y de software en ordenadores remotos a los que los usuarios acceden vía a Internet a través de los dispositivos de su elección"*[1], completando el concepto con *"*(es) *el almacenamiento, tratamiento y utilización de datos en ordenadores a distancia a los que se tiene acceso a través de Internet. Esto significa que los usuarios pueden obtener una capacidad informática casi ilimitada y a voluntad, que no tienen que hacer importantes inversiones de capital para satisfacer sus necesidades y que pueden acceder a sus datos desde cualquier lugar con una conexión a Internet"*[2].

Más concreta es la definición que arroja el Grupo de Trabajo del artículo 29, al establecer: *"cloud computing consists of a set of technologies and service models that focus on the Internet based use and delivery of IT applications, processing capability, storage and memory space"*[3]. Esta delimitación, concebida de forma tecnológicamente neutra, previsiblemente para no limitar la aplicación de las recomendaciones establecidas en la futura evolución del servicio, no recoge las características esenciales que rigen, en la actualidad, la computación en la nube. Sin embargo, coincide, en lo esencial, con la definición establecida en los debates en el seno de la Comisión de las Naciones Unidas

[1] COMISIÓN EUROPEA: "Agenda Digital: Nueva estrategia para impulsar las empresas europeas y la productividad de la administración pública gracias a la computación en nube" (27.09.2012), 2012. Nota de prensa accesible en: http://europa.eu/rapid/press-release_IP-12-1025_es.htm. Último acceso: 08.08.2018.

[2] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Liberar el potencial de la computación en nube en Europa, 2012, COM (2012) 529 final (27.09.2012). Accesible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2012:0529:FIN. Último acceso: 08.08.2018.

[3] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 5/2012 on cloud computing, 2012, 01037/12/EN WP 196 (01.07.2012)", 2012, p. 4. Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Último acceso: 08.08.2018.

para el Derecho Mercantil Internacional[4] y lo establecido por RENGIFO GARCIA[5] y GUTIÉRREZ Y KORN[6].

Parece que la definición más aceptada de la computación en la nube es la establecida por el National Institute of Standards and Tecnology (NIST) de USA. Concibe al *cloud computing* como *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models"*[7]. Por lo tanto, destaca que el modelo de la nube permite el acceso en todas partes bajo conexión a Internet, conveniente y bajo demanda del cliente sobre un conjunto de recursos compartidos y configurables, siendo esencial la accesibilidad rápida con un esfuerzo mínimo en la gestión o la intervención del proveedor del servicio. Es decir, acceso ubicuo, adaptado y bajo demanda en red, con mínima intervención, a recursos configurables compartidos[8].

Siguiendo la propia definición del NIST es necesario abordar, por tanto, las características claves, los modelos de servicio y las formas de implantación de la nube.

---

[4] Define al *cloud computing* como *"servicios de informática (por ejemplo hospedaje y procesamiento de datos) que son suministrados a través de la Internet"*. CNUDMI: "Posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube" - Propuesta del Gobierno del Canadá" 48º Período de sesiones, 2015, p. 3. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V15/040/53/PDF/V1504053.pdf. Último acceso: 08.08.2018.

[5] *"Forma de almacenamiento de información y contenidos digitales en una plataforma intangible, la cual ha surgido con el advenimiento de las nuevas tecnologías"*. RENGIFO GARCÍA, Ernesto: " Computación en la nube", *Revista la propiedad inmaterial,* 2013, nº 17, p. 223.

[6] *"La nube provee recursos de computación en pool que están disponibles según la demanda y accesibles en cualquier momento desde cualquier dispositivo conectado a Internet"*. GUTIÉRREZ, Horacio E. y KORN, Daniel: "Facilitando "the cloud": la regulación de la protección de datos como motor de la competitividad nacional en América latina", *Revista la propiedad inmaterial,* 2014, nº 18, p. 91.

[7] NIST: "The NIST Definition of Cloud Computing", 2011. Accesible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Último acceso: 08.08.2018.

[8] GARCÍA MEXÍA coincide al establecer que el *cloud computing* puede entenderse como la modalidad de prestación de servicios de la sociedad de la información tipo self-service y bajo demanda del cliente, a cuya disposición se pone un conjunto de servicios virtuales, potencialmente escalables según las necesidades del propio cliente, pudiendo prestarse de manera gratuita o mediante el pago por el uso. GARCÍA MEXÍA, Pablo: "Cloud computing: sus implicaciones legales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2010, nº 23, p. 79.

Cinco son las características esenciales que señala el propio NIST[9]:

- Autoservicio bajo demanda del cliente: por el cual el cliente puede, de forma unilateral, decidir sobre las capacidades de computación de forma automática y sin necesidad de interacción interpersonal con el proveedor de servicio.
- Acceso a banda ancha convencional: las capacidades se encuentran disponibles en la red, accediendo a través de mecanismos normales, con las compatibilidades de plataformas que tenga abatibles el cliente, por ejemplo, a través de teléfonos móviles o *tablets*. Se pretende una completa disposición de datos y aplicaciones, en cualquier lugar y desde cualquier equipo, siempre que el usuario, ciudadano y/o empresa disponga de una conexión a Internet.
- Puesta en común de los recursos: los recursos informáticos del proveedor de la computación en la nube se ponen a disposición de múltiples clientes a través de un modelo multi-inquilino, servicios que dependen de las propias necesidades del cliente. Este no conoce la ubicación exacta de los recursos proporcionados, de sus datos ni tiene ningún control. Saber dónde se encuentra y de qué infraestructuras se sirve puede que no tenga relevancia para el desarrollo del servicio en el usuario, pero sí puede tener una especial relevancia jurídica[10]. Sí puede tener conocimiento, según el modelo de implantación, del país o centro de datos en el que opera el proveedor.
- Elasticidad y rapidez en la provisión del servicio, en algunos casos de forma automática, en función de la demanda del consumidor. Las capacidades aparecen, para los clientes habituales, como ilimitadas y están disponibles en cualquier momento. De igual forma, se elimina la posibilidad de medios informáticos infrautilizados.
- Medición del servicio o mensurabilidad: el *cloud computing*, los servicios que ofrece, se controlan automáticamente, con el fin de aprovechar la capacidad y optimizar los recursos. Los recursos se pueden monitorizar y supervisar, dando transparencia al servicio utilizado.

[9] NIST: "The NIST Definition of Cloud Computing", 2011, p. 2 Accesible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Último acceso: 08.08.2018.

[10] A modo de orientación al lector, piénsese en la determinación de la jurisdicción y ley aplicable en un conflicto entre usuarios, usuarios finales, proveedores de servicio y subproveedores de servicio.

Junto a estas características esenciales, se han señalado otros rasgos diferenciadores del servicio:

- Desmaterialización: se intenta que la configuración, localización y/o mantenimiento de los medios informáticos sean los menos posibles para los usuarios, ciudadanos o las empresas[11]. Se puede separar el *software* de los sistemas físicos donde se instala, despreocupándose el cliente de los sistemas físicos al ser independiente del *hardware.*
- Pago por uso o coste basado en el consumo real: el usuario, cuando los servicios sean mediante pago, solo tendrá que asumir el costo económico real, en función de las necesidades de capacidad informática[12].
- Los usuarios no tienen que asumir la organización ni la explotación de medios informáticos que tienen gran complejidad, a lo que hay que añadir que no asumen los costes iniciales y fijos que supone la implantación del servicio.
- La computación en la nube, como servicio, se configura en tres capas: equipos físicos, plataformas y aplicaciones informáticas.

Los modelos de computación en la nube o las clases de *cloud* están determinadas por la titularidad del servicio y el control y gestión de los entornos informáticos[13]:

- En el *cloud* público la infraestructura, plataforma y aplicaciones informáticas son administradas por un proveedor de la nube y están a disposición de una pluralidad de clientes, bien sea para los clientes en la nube o para los usuarios finales. Es común que el acceso a la nube se realice a través del Internet público. Por lo tanto, se comparte infraestructura dando un servicio multiusuario. Al optimizarse los recursos por parte del proveedor, suelen tener precios más reducidos, pero generan mayor desconfianza en cuanto al aislamiento de la información y aplicaciones de

[11] Dictamen del Comité Económico y Social Europeo sobre el tema "La computación en nube (cloud computing) en Europa" (Dictamen de iniciativa), 2012 (26.10.2011). Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52011IE1606&from=ES. Último acceso: 08.08.2018.

[12] LÓPEZ JIMÉNEZ, David: "La "computación en la nube" o "cloud computing" examinada desde el ordenamiento jurídico español", *Revista de Derecho,* 2013, nº 40, p. 6.

[13] GARCÍA SÁNCHEZ, Manuel: "Retos de la computación en la nube", *Derecho y Cloud computing*, 2012, p. 41-44; GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 48-53; ALARCÓN FIDALGO, Joaquín: "Cloud computing, responsabilidad y seguro", *Revista Española de Seguros*, 2013, nº 153-154, p. 30-31; y LÓPEZ JIMÉNEZ, David: "La "computación en la nube" o "cloud computing" examinada desde el ordenamiento jurídico español", *Revista de Derecho,* 2013, nº 40, p. 7-8.

los clientes. El carácter público no implica gratuidad del servicio. En resumen, el cliente de la nube pública tiene un grado muy limitado de control y supervisión sobre la actuación del proveedor.

- En la nube privada el cliente es el único usuario del servicio. El *hardware* puede ser gestionado y mantenido por el proveedor de la nube, normalmente a través de un contrato de *outsourcing*, o por la propia organización cliente. De igual forma, puede residir en las instalaciones del cliente o fuera de ellas. Lo característico, por tanto, es que la infraestructura asociada esté restringida a un cliente u organización, no compartida con otro usuario. Otra de las características es la posibilidad de circunscribir el servicio a una red de área local. Al no compartirse recursos con otros clientes, genera mayor confianza en los clientes corporativos, estando aseguradas mediante *firewall*. El modelo permite un elevado control y supervisión en la gestión de la nube. Se aprovecha la flexibilidad y productividad de la nube, siendo la externalización un problema ajeno o menor, si bien, su implementación es cara y existe una excesiva dependencia de las infraestructuras contratadas.
- En la nube comunitaria o compartida la infraestructura tecnológica es compartida por distintos clientes que apelan a un fin específico. Por lo tanto, es característica de organizaciones que comparten requisitos comunes y que requieren servicios similares de computación en la nube. El servicio puede ser restringido a una red de área amplia. Al limitarse los recursos compartidos, sigue generando la confianza de los clientes corporativos. Al igual que la nube privada, puede ser gestionada y mantenida por un proveedor del servicio o por las propias organizaciones, y la infraestructura puede radicar en las instalaciones de la comunidad o fuera de ella.
- *Cloud* híbrida sería una mezcla o composición de las características recogidas para las nubes públicas, privadas y/o comunitarias. Lo clientes, por lo tanto, pueden ser propietarios de unas partes y compartir otras, segregarán los datos y servicios a través de diferentes servicios en la nube, con acceso restringido entre ellos en función de los datos que contengan. GARCÍA DEL POYO[14] resalta que este tipo de nubes suelen ser utilizadas en empresas que necesitan una infraestructura

[14] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 51.

tecnológica simple, que no requieren un alto grado de sofisticación, pero que a su vez puede ser escalable en capacidad en un corto espacio de tiempo.

MARTINEZ FERREIRO[15] destaca la importancia de los entornos *multicloud* como marco único de gestión y monitorización de las distintas nubes, ya sean públicas, privadas, comunitarias y/o híbridas. Los clientes, en función de las necesidades, como la elasticidad o control, entre otros, pueden optar por utilizar diferentes modalidades del servicio, lo que requieren por parte de las organizaciones y/o usuarios un sistema de gestión e interoperabilidad real entre las distintas nubes contratadas y/o establecidas.

Recientemente ha aparecido una nueva modalidad como fusión entre el servicio del *cloud computing* y el conocido como *Internet of Things*, el *fog computing*. Se centra en la manera de almacenar y procesar los datos que residen en la nube y se generan por el Internet de las Cosas. GARNET INC[16] predice que el Internet de las Cosas alcanzará 26 mil millones de unidades conectadas a la nube en 2020. BAR-MAGEN[17] define el *fog computing* como una arquitectura que se basa en la colaboración de los clientes finales y dispositivos de los usuarios para llevar a cabo una gran cantidad de almacenamiento, en la nube, teniendo facultades el cliente de comunicación, control, configuración, medición y gestión a través del Internet. Un ejemplo real, en la actualidad, puede ser la Google Glass[18]. HERNANDEZ DE ROJAS[19] indica que con el *fog computing* se podrán establecer dispositivos realmente inteligentes, dado que se podrá almacenar información y ser programados para mantener conductas e interactuar con el usuario. Habrá que tener presente la evolución del servicio. Sin embargo, los problemas que plantean los datos en

---

[15] MARTÍNEZ FERREIRO, Susana: "La convergencia de cloud pública e híbrida dará paso a entornos multicloud", *A un clic de las Tic*, Telefónica, 2015 (14.07.2015). Accesible en: http://www.aunclicdelastic.com/la-convergencia-de-cloud-publica-e-hibrida-dara-paso-a-entornos-multicloud/. Último acceso: 08.08.2018.

[16] ITBusinessEDGE (Blog): "How the Internet of Things Will Transform the Data Center". Accesible en: http://www.itbusinessedge.com/slideshows/how-the-internet-of-things-will-transform-the-data-center-08.html. Último acceso: 08.08.2018.

[17] BAR-MAGEN, Jonathan: "Fog computing. Introduction to a New Cloud Evolution", *Escrituras silenciadas: paisaje como historiografía*, 2013, p. 111-113.

[18] Para conocer cómo funciona el producto se puede acceder a https://www.google.com/glass/start/.

[19] HERNANDEZ DE ROJAS, Félix: "Fog computing: motor de innovación para el mundo IoT", *A un clic de las Tic*, Telefónica, 2015 (4.02.2015). Accesible en: http://www.aunclicdelastic.com/fog-computing-motor-de-innovacion-para-el-mundo-iot/. Último acceso: 08.08.2018.

la nube serán extrapolables al *fog computing*, dado que emplea el servicio de almacenamiento, gestión y control de la tecnología que ahora estudiamos.

Por último, los modelos de implantación disciernen en las aplicaciones, plataformas o infraestructuras ofrecidas por la contratación del *cloud*[20]:

- Infraestructura como un servicio, *Infrastructure as a Service, IaaS*. Con este modelo se accede a recursos en bruto a través de la nube, es decir, los clientes disponen del acceso al *hardware* que ofrece el proveedor de servicios, según la capacidad que se requiera. Con esta implantación, los usuarios adquieren externamente recursos y equipos para sus operaciones informáticas. Con estos componentes en línea, las organizaciones y/o ciudadanos pueden construir sus propias plataformas tecnológicas. Está más destinada para organizaciones, mediante pago por uso[21].
- Plataforma como servicio, *Platform as a Service, PaaS*. A través del servicio los clientes tienen acceso a una plataforma informática en la que pueden escribir aplicaciones, para ejecutar en la propia plataforma o en otras instancias. Es decir, se posibilita al usuario desarrollar, testear, desplegar, almacenar y mantener sistemas y aplicaciones. Además, puede consistir en el suministro de paquetes de servicios o de aplicaciones. De esta forma, el proveedor de servicios de la nube ofrece lenguajes y herramientas de programación que son gestionadas por él. Como podemos apreciar, es un servicio destinado, principalmente, a usuarios u organizaciones especializadas en el sector IT. Esta plataforma puede estar alojada,

[20] CNUDMI: "Posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube" - Propuesta del Gobierno del Canadá" 48º Período de sesiones, 2015, p. 5. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V15/040/53/PDF/V1504053.pdf. Último acceso: 08.08.2018; MORALES, José Ramón: "Cloud computing: Riesgos corporativos e implicaciones jurídicas", *Actualidad jurídica Aranzadi*, 2013, nº 863, p. 11-14; ALARCÓN FIDALGO, Joaquín: "Cloud computing, responsabilidad y seguro", *Revista Española de Seguros*, 2013, nº 153-154, p. 31; GARCÍA SÁNCHEZ, Manuel: "Retos de la computación en la nube", *Derecho y Cloud computing*, 2012, p. 42; y Dictamen del Comité Económico y Social Europeo sobre el tema "La computación en la nube (*cloud computing*) en Europa" (Dictamen de iniciativa), 2012, 2012/C24/08 (28.01.2012).

[21] Queremos resaltar como muchos servicios de almacenamiento que se ofrecen en Internet, como puede ser Dropbox o Mega, se describen de una forma más efectiva como un servicio *SaaS*, dado que empaquetan el recurso de infraestructura y lo presentan a través de una aplicación que permite alojar una copia de seguridad o compartir archivos. Los recursos más requeridos son servidores, conmutadores, routers y sistemas de almacenamiento.

a su vez, en un modelo *IaaS*[22]. La Comisión de Asuntos Jurídicos para la Comisión de Industria, Investigación y Energía[23] sobre la liberación de nube señala que en este tipo de servicios la responsabilidad de seguridad incumbe en gran medida en el cliente, aspecto muy a tener en cuenta cuando analicemos el clausulado de los contratos de servicios en materia de seguridad.

- El programa informático como un servicio o *software* como servicio, *Software as a Service, SaaS*. Ofrece acceso a una aplicación o aplicaciones de *software* completo a través de un navegador web u otro *software*. Es el modelo de implantación más utilizado por los usuarios finales, dado que los clientes pueden tener acceso, a través de Internet, a aplicaciones y programas informáticos para consumo personal. De esta forma, se reduce o se elimina la necesidad, según los servicios y las necesidades, de instalar un sistema de acceso en las infraestructuras del cliente y permite un amplio acceso a través de distintos dispositivos. Este servicio puede valerse de los modelos de servicios anteriores para su implantación. Los servicios de Gmail o Microsoft Office 365 pueden ser ejemplos de servicios utilizados por clientes finales, aunque también las empresas hacen uso de este servicio para sus tareas de contabilidad, facturación o vigilancia, por ejemplo. En resumen, con este servicio se sustituye instalar los programas informáticos adquiridos en las computadoras o redes, dado que se tiene acceso a las aplicaciones informáticas a través del proveedor de la nube. Los derechos relacionados con los programas utilizados serán considerados en la relación entre el proveedor del servicio en la nube y el cliente. En este caso, la Comisión de Asuntos Jurídicos para la Comisión de Industria, Investigación y Energía[24] sobre la liberación de la nube recoge que la responsabilidad incumbe al proveedor de la nube, dado que es él quien tiene una gestión directa sobre las aplicaciones y servicios de la nube.

---

[22] Son pocos los proveedores de computación en la nube que ofrecen servicios PaaS. Destacan el OpenShift Enterprise 3 (https://enterprise.openshift.com/) y Apprenda (http://apprenda.com/) .

[23] COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA: "Informe sobre la liberación de la computación en la nube en Europa (2013/2063 (INI))", 2013, (24.10.2013), p.23. Accesible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//ES. Último acceso: 08.08.2018.

[24] COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA: "Informe sobre la liberación de la computación en la nube en Europa (2013/2063 (INI))", 2013, (24.10.2013), p.24. Accesible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//ES. Último acceso: 08.08.2018.

Las características, los modelos de servicio y las formas de implantación del *cloud computing* no deben ser óbice para la aplicación del Derecho general, aunque en nuestro estudio nos centremos en el Derecho de contratos, sin perjuicio de una regulación específica que recoja aspectos indisolubles a las propias características del nuevo modelo de servicio. Debe tenerse en cuenta, de igual forma, que una mayor o menor regulación jurídica estará relacionada con las características del servicio contratado, debiendo ser baluarte la libertad de expresión y libertad de contratación entre partes, desde un prisma jurídico político, y la libre competencia y sin restricciones, desde un ámbito económico, teniendo presente los contrapesos de la protección de los consumidores y usuarios, la protección de datos de carácter personal y el eficaz desarrollo económico, social y cultural.

b. Potenciales riesgos de la adopción del *cloud computing*

El *pool* de servicios de la computación en la nube se configura sobre la base de la deslocalización de las actividades contratadas, por consiguiente, la mayoría de los problemas jurídicos que suscita el uso del *cloud computing* superan las fronteras de los estados, incluso las uniones de los mismo, justificando una regulación contractual previa a la contratación de tales servicios. La propia intensidad del problema dependerá de la clase de *cloud* contratado, así como del modelo implantado[25].

Los potenciales riesgos que se han destacado del servicio no debe ser óbice para reconocer las ventajas o beneficios económicos que nos ofrece la implantación de la nube, entre los que destacan la reducción de costes, la inmediatez, la disponibilidad, la escalabilidad, la eficacia y la eficiencia. Incluso, REGINFO GARCÍA[26] nos muestra que la computación en la nube puede ser considerada como una alternativa para combatir la piratería de *software*.

En efecto, desde un punto de vista económico financiero la utilización del *cloud computing* supone un ahorro en costes de capital, al no requerir grandes inversiones en *hardware,* sobre todo por una inversión inicial reducida (no obstante, se traduce en un

[25] Conviene recordar las palabras de Lessig al indicar que serán los profesionales técnicos informáticos quienes en último extremo determinen si una conducta se ajusta a los cánones de la Red, con independencia de las directrices o la regulación que los gobiernos y ordenamientos pudieran establecer. Véase: LESSIG, Lawrence: "El código y otras leyes del ciberespacio", 2001, Taurus, p. 67-89.

[26] REGINFO GARCÍA, Ernesto: "Computación en la nube", *Revista La Propiedad Inmaterial*, 2013, nº 17, p. 224.

incremento de las necesidades existentes para los proveedores del *cloud* y de las empresas y editores que trabajan en el sector para adaptar sus productos a las características del nuevo servicio); el control de costes y beneficios de tipo marginal, al ajustarse a las necesidades de los clientes y tratarse más como un coste de funcionamiento que de inmovilizado; tener una continuidad del servicio ante los cambios de demanda, por la flexibilidad y escalabilidad del servicio; movilidad y disponibilidad de datos y *software*; e incremento de los recursos disponibles por los usuarios y capacidad de recuperación ante desastres o catástrofes informáticas.

La Comisión Europea ensalza el impacto positivo de la implantación de la nube en el crecimiento y el empleo, no solo en los empleos directamente relacionados con el sector de actividad en cuestión, que Microsoft señala que creció un 24% anual hasta el año 2015 con una creación total de 1,4 millones de empleos relacionados en Europa[27], sino en la contribución a reducir los costes fijos en las organizaciones, sobre todo en las PYMES, que permitirá la creación, desarrollo y aumento de productividad del tejido empresarial[28]. Como señalan CUESTA SAINZ, ALONSO, TUESTA y FERNÁNDEZ DE LIS[29], los proveedores ofrecen servicios de la nube a unos precios reducidos gracias a la demanda agregada de los clientes, la industrialización de sus procesos y la optimización del parque tecnológico. Por lo tanto, el hecho de que los proveedores se centren en la prestación de una gama reducida de servicios, sin grandes diferencias, permite industrializar sus procesos, pudiendo reducir los gastos de administración y mantenimiento de las infraestructuras tecnológicas. En consecuencia, todos los usuarios podrán acceder a un nivel de servicios que antes estaba disponible solo para las grandes organizaciones y para las economías más desarrolladas, presentando oportunidades para las empresas y usuarios

[27] ANDERSON, Cushing y GANTZ, John F.: "Climate Change: Cloud´s Impacto on IT Organizations and Stafflin", *Microsoft White Paper*, 2012, p. 4. Accesible en: https://news.microsoft.com/download/presskits/learning/docs/IDC.pdf. Último acceso: 08.08.2018.

[28] COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA: "Informe sobre la liberación de la computación en la nube en Europa (2013/2063 (INI))", 2013, (24.10.2013), p.8. Accesible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//ES. Último acceso: 08.08.2018.

[29] CUESTA SAINZ, Carmen; ALONSO, Javier; TUESTA, David; FERNÁNDEZ DE LIS, Santiago: "El desarrollo de la industria del cloud computing: impactos y transformaciones en marcha", *BBVA Research – Observatorio de Economía Digital*, 2014, (04.07.2014). Accesible en: https://www.bbvaresearch.com/publicaciones/el-desarrollo-de-la-industria-del-cloud-computing-impactos-y-transformaciones-en-marcha/. Último acceso: 08.08.2018.

particulares, propiciando una democratización de los servicios informáticos y mayor inclusión social. Sin embargo, hay discordia de opiniones en este último argumento, entre ellos los vertidos en el seno de la propia Comisión Europea[30], si la propia implantación de la nube no va ligada al desarrollo de las infraestructuras tecnológicas generales, dado que la falta o insuficiencia de conexión de banda ancha podría agrandar la brecha digital entre las zonas rurales y urbanas, dificultando la cohesión territorial y el crecimiento económico.

En el marco de la CDNUMI[31] se ha expuesto, además, como principales efectos macroeconómicos positivos una contratación predecible, la certidumbre en torno al uso de la nube, la posibilidad de unas normas que permitan la interoperabilidad entre los productos e interfaces de la nube, una mejor definición del servicio y la existencia de una legislación adecuada para proteger los datos personales y la confidencialidad.

Estos beneficios, como se observa principalmente económicos, tienen como contrapesos los potenciales riesgos que se asumen en la utilización del *cloud computing*, derivados de la propia naturaleza y el funcionamiento intrínseco del servicio. Los principales riesgos de la tecnología del *cloud computing* están relacionados con las áreas de autentificación, seguridad de los datos y privacidad, la interconexión con los sistemas internos, la disponibilidad de los sistemas, la continuidad del negocio, la propiedad de los contenidos y otros requisitos legales[32].

La expansión en el uso actual de estos servicios informáticos y la necesidad de que dichos servicios se ajusten de manera rápida a las necesidades de los usuarios puede propiciar problemas en el funcionamiento del tráfico de Internet, y por ende del servicio. Relacionado con este problema está el hecho de la fragilidad del funcionamiento del *cloud computing*, riesgo intrínseco por su dependencia a una conexión de red. De esta forma,

---

[30] COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA: "Informe sobre la liberación de la computación en la nube en Europa (2013/2063 (INI))", 2013, (24.10.2013), p.8. Accesible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//ES. Último acceso: 08.08.2018.

[31] CNUDMI: "Posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube" - Propuesta del Gobierno del Canadá" 48º Período de sesiones, 2015, p. 6. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V15/040/53/PDF/V1504053.pdf. Último acceso: 08.08.2018

[32] CHOU, David C.: "Cloud computing risk and audit issues", *Computers Standards & Interfaces*, 2015, p. 140.

los incidentes técnicos, la delincuencia informática o las decisiones económicas ponen de relieve la dependencia del servicio a decisiones fuera del marco técnico. Riesgos que, como exhibe el Comité Económico y Social[33], se ven incrementados por la resiliencia de la red y el deseo de los usuarios de contar con una respuesta en corto espacio de tiempo. ALARCÓN FIDALGO, incluso, considera que es inevitable un previsible deterioro de la escalabilidad por un uso masivo de los servidores, provocando una sobrecarga de los mismos[34]. Sin embargo, vivir en servidores externos es la razón ser del *cloud*. Gracias a ello, tras el terremoto que asoló Costa Rica el 5 de septiembre de 2012, y que supuso la interrupción de las comunicaciones tradicionales por derrumbe de las infraestructuras de comunicaciones del país, los ciudadanos costarricenses pudieron estar informados gracias a que Teletica (televisión nacional) había implantado recientemente los servicios de la nube[35].

Problema sustancialmente técnico es la seguridad de los datos, principalmente sobre la base de la externalización del servicio, incrementándose por la posible descentralización de los datos. La disponibilidad y la confidencialidad se antojan fundamentales en la regulación del servicio. Con el uso de la nube, los datos o ficheros residen en unos servidores gestionados por terceros, que deberían asumir todas las medidas de seguridad idóneas para poder garantizar la integridad de nuestros datos. La seguridad y confidencialidad, como veremos, son especialmente relevantes cuando abordemos la protección de datos personales. ENISA[36] explica que la seguridad *"constituye una prioridad para muchos clientes en nube"* determinando que *"los clientes toman las decisiones relativas a la adquisición basándose en el renombre del proveedor*

[33] Dictamen del Comité Económico y Social Europeo sobre el tema "La computación en nube (cloud computing) en Europa" (Dictamen de iniciativa), 2012 (26.10.2011). Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52011IE1606&from=ES. Último acceso: 08.08.2018.

[34] ALARCÓN FIDALGO, Joaquín: "Cloud computing, responsabilidad y seguro", *Revista Española de Seguros*, 2013, nº 153-154, p. 32.

[35] LYNDERSAY, Mark: "Microsoft evangelises the cloud", *Guardian (edición digital)*, noticia de 25.10.2012. http://www.guardian.co.tt/business-guardian/2012-10-24/microsoft-evangelises-cloud. Ultimo acceso: 08.08.2018.

[36] ENISA (European Network and Information Security Agency): "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

en cuanto a confidencialidad, integridad y resistencia de fallos, así como en los servicios de seguridad", siendo, incluso, más cautelosos que cuando se contratan servicios tradicionales. Debe valorarse que con los servicios de *cloud* las organizaciones pueden lograr protecciones solo disponibles, si se utilizaran infraestructuras internas, a organizaciones de gran tamaño, dado que requieren una inversión inicial y un mantenimiento difícilmente asumible para la mayoría de las empresas, instituciones y usuarios. ALERTLOGIC[37], en el último informe publicado, muestra una tasa de incidentes de seguridad de un 51% más alta en los *datacenters* locales que en los servicios de nube, teniendo la nube pública que soportar aproximadamente (en promedio) alrededor de 400 incidentes de seguridad. Sin embargo, al no tener un control sobre los datos, las instituciones gubernamentales pueden liberar operaciones que pueden poner en alto riesgo la seguridad y la disponibilidad de los archivos. Sirva de ejemplo la operación contra Megaupload, en enero de 2012, auspiciada por el Departamento de Estado de USA, el FBI y diferentes autoridades internacionales[38] o la filtración del ex-técnico de la Agencia Nacional de Seguridad (NSA) estadounidense, Edward Snowden, de cómo el gobierno de los Estados Unidos de América, con la benevolencia de los grandes proveedores de los servicios de comunicaciones, "espiaban" a los usuarios de los servicios sin mediar orden judicial previa, revelación que ha hecho cambiar la política de privacidad de datos de las principales compañías de servicios[39]. ALI, KHAN,

[37] ALERTLOGIC: "Cloud security report. Research on the Evolving State of Cloud Security", 2017, p. 7. Accesible en (bajo petición): https://www.alertlogic.com/resources/cloud-security-report-2017. Último acceso: 08.08.2018.

[38] Puede obtener más información: RODRÍGUEZ, Sergio: "El FBI cierra Megaupload, una de las mayores webs de intercambio de archivos", *El Mundo.es (edición digital),* noticia de 20.01.2012 http://www.elmundo.es/elmundo/2012/01/19/navegante/1327002605.html, ultimo acceso: 08.08.2018; y Redacción BBC: "Cuatro claves del cierre de Megaupload", *BBC Mundo (edición digital),* noticia de 20.01.2012. http://www.bbc.com/mundo/noticias/2012/01/120119_megaupload_clave_tsb.shtml, ultimo acceso 08.08.2018.

[39] Para más información puede estudiar: EUROPA PRESS: "Apple, Facebook y Google avisarán cuando el Gobierno de EEUU pretenda acceder a datos", *El Mundo.es (edición digital)*, noticia de 05.05.2014, http://www.elmundo.es/tecnologia/2014/05/05/53676c38e2704eb0068b4579.html, último acceso: 08.08.2018; y TIMBERG, Craig: "Apple, Facebook, others defy authorities, increasingly notify users of secret data demands after Snowden revelations", *The Whashington Post (digital)*, noticia de 01.05.2014, http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html?hpid=z1, último acceso: 08.08.2018.

VASILAKOS[40] reiteran como los riesgos de las infraestructuras de IT convencional suelen ser diferentes a los que acaecen en la nube, tanto por la naturaleza como por la intensidad de ambos. El autoservicio y la multi-tenencia ayudan a los riesgos asociados a la visibilidad de los datos de otros usuarios y el acceso no autorizado a la interfaz de gestión. La ONTSI recomienda, al objeto de prevenir los riesgos expuestos, estudiar la información que se quiere llevar a la nube, el sector a qué pertenece, la familia (modelo de implantación) que se va a contratar y la criticidad del proceso de negocio que soportará la nube[41]. Por lo tanto, será esencial atender a las cláusulas contractuales que se establezcan con el proveedor del *cloud computing.*

El desarrollo en la prestación del servicio ha propiciado la posición dominante de diferentes empresas[42] con los riesgos inherentes que supone tener dicha posición dominante, entre otros en la imposición de cláusulas contractuales. La Comisión de Industria, Investigación y Energía hace patente el riesgo que presupone que un número limitado de proveedores ofrezcan los servicios en la nube a los consumidores, orientando su utilización en nube privada, al crear una base de consumidores cautivos y acumulando una cantidad considerable, y cada vez más elevada, de datos del usuario[43]. A lo que habría que añadir la carencia de parques de servidores en territorio europeo. De igual forma, esta concentración de volumen, visibilidad y relevancia de datos, sobre todo vinculada con los grandes servidores, constituye un objetivo atractivo para los ataques informáticos. El número limitado de proveedores, con una cantidad ingente de información, aumenta la eficacia, pero aumenta también las posibilidades o probabilidades de pérdidas de los datos ante situaciones catastróficas, puntos centralizados de datos o de acceso de información por parte de terceros.

---

[40] ALI, Mazhar; KHAN, Samee U.; y VASILAKOS, Athanasios V.: "Security in cloud computing: Opportunities and challenges", *Information Sciences*, 2015, p. 361.

[41] ONTSI: "Cloud Computing. Retos y Oportunidades", *Observatorio Nacional de las Telecomunicaciones y de la SI,* 2012, mayo, p. 63-64. Accesible en: http://www.ontsi.red.es/ontsi/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf. Último acceso: 08.08.2018.

[42] Algunos de los dispositivos o servicios informáticos que habitualmente utilizamos están necesariamente vinculados a un proveedor de servicios. Sucede así, por ejemplo, con los productos Apple y su vinculación con iCloud, Facebook con su red social o Google con su servicio de Gmail.

[43] COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA: "Informe sobre la liberación de la computación en la nube en Europa (2013/2063 (INI))", 2013, (24.10.2013), p.5. Accesible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//ES. Último acceso: 08.08.2018.

La portabilidad de los datos y la dificultad de determinar la regulación aplicable son los dos principales riesgos que resaltan las Instituciones que se han aventurado al estudio del *cloud computing*, así como la doctrina. La portabilidad se muestra como requisito necesario para que los usuarios no queden cautivos de un proveedor de la nube, pudiendo transferir los recursos almacenados de un prestador a otro. En este sentido, se plantea como necesario el uso de *open standards*, así como garantizar la interoperabilidad de los servicios y aplicaciones. Por lo tanto, el problema de la portabilidad se presenta como un riesgo no solo técnico, sino también comercial.

Respecto al segundo de los problemas destacados, el propio carácter internacional del servicio, la deslocalización de los datos y la falta de una gobernanza internacional propician que no exista una autoridad de control que vele por la regulación del servicio, así como organismos que puedan solucionar los diferentes conflictos que se generan entre usuarios y proveedores de servicio, entre otros. En la nube, sobre todo con los citados proveedores "gratuitos", puede ser difícil, salvo que se recoja en la propia contratación, determinar dónde están situados los servidores, dónde residen los datos, lo que dificulta determinar la ley aplicable. Con la actual regulación parece haberse solventado, al menos en parte, la consideración de si la ley aplicable es la del cliente, propietario de la información, o aquella donde residen los servidores del proveedor del servicio. Este carácter internacional tiene especial importancia respecto a la protección de los datos personales, tras la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y los derechos de autor ante los ataques actuales que están sufriendo en dicha materia. Aunque parezca recurrente, es más viable, como señala GUTIÉRREZ y KORN[44], que un proveedor de la nube cumpla, de forma global, las exigencias legales que se impongan en los distintos ordenamientos en los que opera, dado que resulta sumamente complicado que los países adopten reglas idénticas de protección.

[44] GUTIÉRREZ, Horacio E. y KORN, Daniel: "Facilitando "the cloud": la regulación de la protección de datos como motor de la competitividad nacional en América latina", *Revista la propiedad inmaterial,* 2014, nº 18, p. 103.

Muchos de estos riesgos potenciales los señala el Grupo de Trabajo del artículo 29 en su opinión 05/2012, de 1 de julio[45]. En concreto, viene a hacer referencia a los problemas de interoperabilidad y los problemas de transferencia de datos y documentos, lo que llevaría a quedar cautivos de un solo proveedor de servicios; la merma de la integridad de los sistemas, por emplearse infraestructuras que requieran sistemas y recursos compartidos; los problemas con la confidencialidad de los datos, más si cabe ante servidores que no se encuentren dentro de la UE, EEE o países asimilados; y la disminución del control, por la complejidad de los servicios y la externalización de los mismos.

La tecnología actual nos permite interactuar en la nube a través de dispositivos móviles. Los recursos limitados de estos, como la baja potencia de procesamiento, la menor capacidad de almacenamiento, la energía limitada y la dispar conexión a Internet, son condicionantes a la hora de evaluar su interactuación con la nube. El nuevo paradigma MCC permite a los usuarios acceder y gestionar sus aplicaciones y datos a través de Internet, solventando las anteriores limitaciones sin necesidad de actuar con grandes máquinas computacionales. ALI, KHAN, VASILAKOS[46] concluyen que el MCC tiene su base en el *cloud computing* tradicional, por lo que todos los riesgos inherentes a la nube son heredados en el nuevo paradigma. Sin embargo, por su propia configuración móvil y las características intrínsecas, los principales riesgos asociados se relacionan con la seguridad de los dispositivos móviles: seguridad de aplicaciones móviles, la privacidad del usuario, la autentificación y la seguridad de los datos.

En resumen, los beneficios que se han asociado al uso del *cloud computing* como la respuesta a las necesidades y presupuestos de las entidades, la mayor flexibilidad, la mejor utilización de los recursos, la mejora en eficiencia y mayor agilidad, el acceso a las nuevas tecnologías, la mejora de la seguridad, la reducción de los costes, la transformación de costes fijos en costes de funcionamiento y la mejor colaboración; deben contrarrestarse con los potenciales riesgos que pueden sufrir los clientes y/o usuarios, a saber, riesgos económicos, de pérdida de control de datos, de prácticas de seguridad inadecuadas del proveedor, acceso no autorizado a la nube, flujo transfronterizos de datos, preservación

[45] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 5/2012 on cloud computing, 2012, 01037/12/EN WP 196 (01.07.2012)", 2012. Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Último acceso: 08.08.2018.

[46] ALI, Mazhar; KHAN, Samee U.; y VASILAKOS, Athanasios V.: "Security in cloud computing: Opportunities and challenges", *Information Sciences*, 2015, p. 379.

de los datos, pérdida de información, acceso no autorizado a la información o al procesamiento, así como los relacionados de índole jurídica, que abordaremos a lo largo del presente trabajo.

Capítulo II - CONTRATOS INFORMÁTICOS Y POR MEDIOS ELECTRÓNICOS. a. Qué son los contratos informáticos y los contratos por medios electrónicos. b. Los bienes informáticos: definición. c. La regulación actual de los contratos electrónicos. d. Principios comunes y específicos en el marco del comercio electrónico. e. En relación con el contrato del *cloud computing*.

CAPÍTULO II – CONTRATOS INFORMÁTICOS Y POR MEDIOS ELECTRÓNICOS

a. Qué son los contratos informáticos y los contratos por medios electrónicos

La expansión de la red y la democratización de los medios informáticos y electrónicos han propiciado que numerosas actividades que en tiempos anteriores realizábamos en presencia de las partes y en soporte material, principalmente papel, ahora se realicen a través de estos nuevos medios. En un análisis de ADICAE[47] sobre consumidores españoles, ya en 2014 destacaba que el 74% de los encuestados afirman haber contratado alguna vez a través de un servicio a distancia, siendo Internet el medio preferido por los usuarios para comprar a distancia o contratar (81,42% de la muestra del estudio). El estudio realizado por el OBSERVATORIO CETELEM[48] aporta que el porcentaje de consumidores que declara haber realizado al menos alguna compra online cada 15 días, en 2017, es de 21%, teniendo un gasto medio anual de 1.954 €. De esta forma, el mercado electrónico, donde se opera a través de computadoras y, de forma común, a distancia, supone un mercado globalizado en el que se concretan las operaciones de compra y venta, principalmente, con las fases intermedias de negociación, intercambio de documentos, información precontactual… En este marco de relaciones, se hace necesario un instrumento legal que obligue a los participantes, no siempre consumidores en el sentido normativo del término, al cumplimiento de las obligaciones contraídas, así como en el caso de incumplimiento interpelar su cumplimiento. Este instrumento no es otro que el contrato. Así lo destaca, entre otros, DÍAZ BRITO[49] al decir *"no cabe duda de que el centro neurálgico en torno al que gira en este ámbito es el contrato y la contratación celebrados a través de medios telemáticos, en particular y por el momento, a través de internet"*. Y es que, parafraseando a ILLESCAS ORTIZ[50], dentro de la contratación electrónica debe tenerse como principios universales la equivalencia funcional de los actos empresariales, la no alteración del derecho preexistente en las obligaciones privadas

[47] ADICAE: "Análisis de la contratación y compra a distancia y sus principales problemas para los consumidores", *Proyecto: Consumidores 2014. Retos y mejoras en sus derechos a la hora de contratar y en su defensa colectiva,* 2014, p. 4-5. Accesible en: http://blog.adicae.net/consumidores-2014/files/2014/12/InformeADICAEFinalFinal.pdf. Último acceso: 08.08.2018.

[48] OBSERVATORIO CETELEM: "La era del "marketplace"", *eCommerce,* 2017, p. 23 y 30.

[49] DÍAZ BRITO, Francisco Javier: "Contratación electrónica: ¿Camino del laberinto?", *Boletín Aranzadi Civil-Mercantil*, 2001, núm. 23/2001, p. 1.

[50] ILLESCAS ORTIZ, Rafael: *Derecho de la contratación electrónica*, 2000, Civitas, p. 46.

y en los contratos establecidos por los medios materiales, la buena fe, la libertad en materia de contratación y, por supuesto, la neutralidad en el uso de las nuevas tecnologías.

En primer lugar, antes de preguntarnos por la calificación del contrato realizado por vía electrónica y por el contrato informático, se hace necesario definir y diferenciar ambos conceptos, y por ende, las categorías jurídicas contractuales.

En el estudio de la contratación electrónica se tendió a confundir los términos contratos informáticos y contratos por medios electrónicos, como dice APARICIO VAQUERO[51], fruto de la imprecisión terminológica, porque la definición de ambos conceptos ha estado siempre delimitada, concibiéndose en los estudios recientes suficientemente afianzadas y diferenciadas las realidades. De esta forma, se utilizaba un concepto amplio de los contratos informáticos, incluyendo aquellos que tenían por objeto los bienes y servicios informáticos y los contratos en los que, independientemente del objeto, se concluía los contratos a través de medios electrónicos o informáticos. Sin embargo, no es solo fruto de la laxitud en el empleo de la terminología adecuada, MENÉNDEZ MATO[52] hace hincapié en dos causas, principalmente: la primera de ellas relacionada, inevitablemente, con la rapidez de la revolución electrónica en los últimos años y la tardanza en su adaptación del campo jurídico, y en segundo lugar, no menos importante, vinculado al propio funcionamiento del mercado y de la economía general, pues, la mayoría de los conceptos tratados en los conceptos jurídicos estudiados en nuestra línea de investigación tienen un profundo contenido y carácter económico. Por lo tanto, la relación e interacción, con las amplias posibilidades, entre Internet y Derecho ha dado lugar a la generación y empleo de términos que no se han utilizado de manera uniforme[53].

---

[51] APARICIO VAQUERO, Juan Pablo: "Contratación informática y outsourcing", *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 2002, Comares, p. 5-6.

[52] MENÉNDEZ MATO, Juan Carlos: "Aspectos teóricos: Concepto. Validez y clasificación", *El contrato vía Internet*, 2005, J.M. Bosch editor, p. 157.

[53] MADRID PARRA señala que *"se trata de un proceso de depuración terminológica paralelo a la fijación misma de los ámbitos de relación entre Derecho y aplicación de los nuevos avances tecnológicos"*. De esta forma, no solo se requiere una delimitación conceptual de los términos actuales, sino la creación de nuevos conceptos y nuevos términos que se adapten a las nuevas realidades jurídicas y tecnológicas. Proceso, resalta MADRID, que debe ser liderado por la industria y los operadores económicos y jurídicos. MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 74.

Muy oportuna nos parece la delimitación que establece MENÉNDEZ MATO[54] de las denominaciones relacionadas en la materia. Parte del concepto de contrato informático, considerando como tal a la contratación que tiene como objeto un bien o un servicio de naturaleza informática[55]. Por lo tanto, lo determinante para clasificar la relación contractual como informática es atender al objeto del contrato, siendo, en principio, indiferente el tipo contractual o la naturaleza material o inmaterial del objeto[56]. DÁVARA RODRÍGUEZ, incidiendo en los elementos esenciales de la contratación informática, establece que *"el análisis de la contratación informática lleva al estudio de los diferentes tipos de relaciones y contratos surgidos en torno al comercio de bienes y servicios informáticos"*[57]. La definición aportada por la doctrina podría ser más concisa, especificando la necesidad de materialidad o inmaterialidad del objeto, e incluso exigiendo que el contrato sea realizado por medios electrónicos y/o telemáticos. En nuestro trabajo, se empleará el concepto de contrato informático en su máxima amplitud, es decir, atendiendo a la naturaleza informática del objeto.

Los contratos por medios electrónicos o los contratos electrónicos se delimitan por los medios que se emplean para la conclusión de los contratos, siendo estos procedimientos o elementos electrónicos. DÁVARA RODRÍGUEZ, y así parece coincidir la mayoría de la doctrina[58], amplía la definición anterior considerando

---

[54] MENÉNDEZ MATO, Juan Carlos: "Aspectos teóricos: Concepto. Validez y clasificación", *El contrato vía Internet*, 2005, J.M. Bosch editor, p. 158-170.

[55] En esta definición coinciden BARRIUSO RUIZ (BARRIUSO RUIZ, Carlos: "La formación del contrato electrónico", *La contratación electrónica*, 2002, Dykinson, p. 182), MADRID PARRA (MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 9-11) y DÁVARA RODRIGUEZ (DÁVARA RODRÍGUEZ, Miguel Ángel: "El comercio electrónico y la contratación electrónica", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi, p. 261).

[56] Más complejo puede ser definir "informática". Atendiendo al concepto que nos otorga la Real Academia Española, se delimita informática al *"conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras"*. Más ortodoxo es el término en manos de FROSINI, al establecer la informática como el proceso de memorización artificial de datos por medio de impulsos electromagnéticos en un soporte físico. FROSINI, Vittorio: *Informatica, diritto e società*, 1992, Giuffrè, p. 341.

[57] DÁVARA RODRÍGUEZ, Miguel Ángel: "El comercio electrónico y la contratación electrónica", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi, p. 39.

[58] Puede verse, también, PLAZA PENEDÉS, Javier: "El marco jurídico de la contratación electrónica", *Comercio, Administración y Registros Electrónicos*, 2009, Thomson Reuters, p. 143 y BERROCAL LANZAROT, Ana Isabel: "Perfección del contrato en la Ley 24/2002, de 11 de julio, de Servicios de la

contratación electrónica aquella que *"se realiza mediante la utilización de algún elemento electrónico cuando este tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo"*[59]. Por lo tanto, se refuerza la importancia de los medios electrónicos al ser relevante el empleo del medio no solo para la conclusión de la contratación[60]. Sin embargo, hay quien mantiene, como MORENO NAVARRETE[61], como requisito necesario que el medio electrónico trasmita la prestación del consentimiento[62]. En similares términos define RECALDE CASTELLS[63] el contrato electrónico.

Se han asimilado los conceptos de contratos electrónicos y contratos telemáticos, dada la frecuencia en el que los contratos electrónicos se concluyen a distancia. Sin embargo, no es necesaria esta vinculación, pudiendo los contratos realizados a través de medios electrónicos perfeccionarse en presencia física de las partes[64]. Siguiendo con este posicionamiento, los contratos electrónicos abarcarían, por tanto, no solo aquellos que se perfeccionan a través de ordenadores. Como posteriormente veremos, el concepto entraba

---

Sociedad de la Información y de Comercio Electrónico: la unificación de criterios", *Revista de Contratación Electrónica*, 2009, núm. 100, p. 12.

[59] DÁVARA RODRÍGUEZ, Miguel Ángel: "El comercio electrónico y la contratación electrónica", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi, p. 190.

[60] MAS BADÍA viene a establecer que para considerar que un contrato se ha celebrado por medios electrónicos es necesario que la oferta y la aceptación se hayan producido por esos medios. Señalando que si alguno de estos trámites se han desarrollado *off line*, no podrán considerarse contratos electrónicos en sentido estricto, lo que no impide que se le aplique la normativa especial a aquellos actos que se hayan desarrollado por las nuevas tecnologías (MAS BADÍA, María Dolores: "El contrato electrónico de seguro", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2015, núm. 38 Mayo-Agosto, p.91).

[61] MORENO NAVARRETE, Miguel Ángel: "Los fundamentos del contrato electrónico", *DERECHO-e Derecho del Comercio electrónico*, 2002, Marcial Pons, p. 32.

[62] Dispone, expresamente: *"solamente nos interesa que a través de dichos medios puedan transmitirse la escritura, la voz o las imágenes además de la combinación de las mismas, en su caso, como medios de prestación del consentimiento"*.

[63] RECALDE CASTELLS, Andrés: "Comercio y Contratación electrónica", *Informática y Derecho – Revista Iberoamericana de Derecho informático*, 1999, núm. 30-31-32, p. 39.

[64] Por ejemplo, cuando acudimos a algunos grandes almacenes podemos acceder al catálogo de productos que ofrece, pudiendo concluir la compra del bien o servicio seleccionado a través de los equipos electrónicos ofrecidos por la entidad. En España, posiblemente, el sector que primero implantó los medios electrónicos en presencia de las partes para la contratación de servicios fue el ferroviario, las denominadas "autoventas" a través de máquinas de venta de billetes en las estaciones. No es de esta opinión ILLESCAS ORTIZ, que establece que el comercio electrónico siempre se produce entre ausentes (ILLESCAS ORTIZ, Rafael: "Los principios generales del Derecho del comercio electrónico", *Derecho de la Contratación Electrónica,* 2009, Civitas, p.34).

en contradicción con muchas definiciones legales que se realizaban y se realizan de contratos electrónicos, que suelen excluir, entre otros, el empleo del fax y el telex. Por lo tanto, aunque atendiendo a la definición el término englobaría cualquier empleo de medios electrónicos, parece que para emplear la locución electrónica es necesario valerse de un tratamiento o almacenamiento de datos.

b. Los bienes informáticos: definición

Desde una concepción amplia, podemos determinar que son los elementos que conforman el *hardware* de un ordenador, así como los periféricos asociados a su principal y los equipos directamente relacionados con el uso del ordenador central y sus periféricos, teniendo corporeidad y siéndole aplicable, como bien mueble, toda normativa relacionada con estos; y todos aquellos bienes inmateriales que dictan el tratamiento de la información, conformando el soporte lógico[65]. La definición más intuitiva de *software* puede ser aquella que la relaciona con la parte lógica del sistema[66]. Tratando el concepto de *software*, la OMPI[67], así como el cuerpo legislativo que regula la propiedad intelectual, entre ellos el Real Decreto Legislativo 1/1996, de 12 de abril, establecen que se compone del programa de ordenador en sí mismo, la descripción del programa y el material de apoyo. Por lo tanto, aunque el objeto principal sea un bien inmaterial, como anteriormente hemos reseñado, no debe obviarse que la descripción o el material de apoyo sí puede tener corporeidad.

La dificultad que entraña estudiar la contratación del *software* no reside tanto en la definición sino en, como señala BARRIUSO RUIZ[68], los diferentes medios a través de los cuales puede obtenerse, gracias sobre todo a la aparición de Internet, así como las

[65] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi, p. 260.

[66] La RAE define el *software* como *"conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora"*.

[67] Es especialmente relevante el Anexo 1C del Acuerdo de Marrakech por el que se establece la Organización Mundial del Comercio, firmado en Marrakech, Marruecos, el 15 de abril de 1994, conocido como el Acuerdo sobre los ADPIC. Accesible en: http://www.wipo.int/treaties/es/text.jsp?file_id=305906. Último acceso: 06.12.2015.

[68] BARRIUSO RUIZ, Carlos: "La formación del contrato electrónico", *La contratación electrónica*, 2002, Dykinson, p. 186.

diferentes formas de adquisición, por ejemplo, a través del arrendamiento de los servicios u obras, la cesión de derechos de cesión o mediante licencia.

Dentro del objeto de los contratos informáticos se incluyen los servicios informáticos, considerando a aquellos los que están vinculados al tratamiento de la información y posean una marcada asistencia a la propia actividad informática.

En resumen, y utilizando el concepto empleado por APARICIO VAQUERO[69], el contrato informático es aquel que tiene por objeto una prestación informática. Esta puede ser la definición más práctica, dado que muchas veces los usuarios, empresas y/o administraciones contratan una mezcla de bienes materiales e inmateriales, siendo el objeto de contrato difícil de delimitar.

c. La regulación actual de los contratos electrónicos

Realizaremos un estudio de las diferentes disposiciones normativas para aproximarnos a la regulación de los contratos electrónicos, con la finalidad de adquirir la suficiente destreza para, posteriormente, analizar los principios del comercio electrónico.

Debemos partir de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)[70]. Aunque la referencia al contrato electrónico es directa, de forma expresa solo hace mención, incluyendo contratación electrónica, en los Considerando 34, 35, 36, 37 y 38, en el artículo 1.2 y sobre todo en la Sección 3ª del Capítulo II (artículos de 9 al 11). Sí se echa de menos que no se recoja qué debe considerarse contrato electrónico en el artículo 2, "definiciones". Es importante resaltar como la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la

[69] APARICIO VAQUERO, Juan Pablo: "Contratación informática y outsourcing", *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 2002, Comares, p. 6.

[70] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32000L0031 y https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295. Último acceso: 08.08.2018.

información[71] define en el artículo 1.b.ii) qué debe entenderse "por vía electrónica". A los efectos de la Directiva, se relaciona exclusivamente con los servicios enviados y recibidos mediante *"equipos electrónicos de tratamiento y de almacenamiento de datos"*, canalizándose a través de medios electromagnéticos.

Como iniciativas del denominado Mercado Único Digital[72], se han publicado las Propuestas de Directiva del Parlamento Europeo y del Consejo, de 9 de diciembre de 2015, relativa a determinados aspectos de los contratos de suministro de contenidos digitales[73] y de Directiva del Parlamento Europeo y del Consejo, de 9 de diciembre de 2015, relativa a determinados aspectos de los contratos de compraventa en línea y otras ventas a distancia de bienes[74]. En la primera de las propuestas, se define bienes informáticos para la denominada nueva era digital. Así, establece en el artículo 2 qué se considera contenido digital[75]. Pero más importante puede ser la determinación de "entorno digital", considerado como el *"hardware, contenidos digitales y cualquier conexión a la red en la medida en que se encuentren bajo el control del usuario"*. Respecto a la propuesta relativa sobre la compraventa en línea, tras declarar en el Considerando (3) que *"el comercio electrónico es el principal motor del crecimiento en el marco del Mercado Único Digital"*, recoge en el artículo 2.e la definición del contrato de compraventa a distancia, estableciendo que es *"todo contrato de compraventa celebrado siguiendo un plan organizado a distancia sin la presencia física simultánea del vendedor y del consumidor, por medio del uso exclusivo de uno o más medios de*

[71] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32015L1535. Último acceso: 08.08.2018.

[72] Para más información se puede acceder al comunicado de prensa de la Comisión Europea. COMISIÓN EUROPEA: "Un mercado único digital para Europa: la Comisión establece 16 iniciativas para conseguirlo" (06.05.2015), 2015. Nota de prensa accesible en: http://europa.eu/rapid/press-release_IP-15-4919_es.htm. Último acceso: 08.08.2018.

[73] Accesible en: http://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-634-ES-F1-1.PDF. Último acceso: 08.08.2018.

[74] Accesible en:https://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-635-ES-F1-1.PDF. Último acceso: 08.08.2018.

[75] Considera, la normativa, como contenido digital: *" a) datos producidos y suministrados en formato digital, por ejemplo vídeo, audio, aplicaciones, juegos digitales y otro tipo de software, b) servicio que permite la creación, el tratamiento o el almacenamiento de los datos en formato digital, cuando dichos datos sean facilitados por el consumidor, y c) servicio que permite compartir y cualquier otro tipo de interacción con datos en formato digital facilitados por otros usuarios del servicio."*

comunicación a distancia, incluido internet, hasta el momento en que se celebra el contrato, con inclusión de ese momento". Por lo tanto, y en términos generales, las Propuestas hacen eco del núcleo fundamental desarrollado por la doctrina para la consideración de un contrato como electrónico, incorporando Internet directamente como medio propicio de la contratación a distancia.

En España, la trasposición de la Directiva sobre el comercio electrónico se tradujo en La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[76]. Destaca, en primer lugar, el empleo continuo del concepto de contrato o contratación electrónica. Entre las referencias expresas, propositiva es la definición recogida en el Anexo. En el apartado h) indica expresamente (se entenderá por) "*"contrato celebrado por vía electrónica" o "contrato electrónico": todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones*." Este concepto debe vincularse de forma obligatoria con el apartado a) del Anexo, que define los servicios de la sociedad de la información, determinando en su subapartado 1 *"la contratación de bienes o servicios por vía electrónica"* y "*el suministro de información por vía telemática"*. De la definición se extraen, como características básicas, que es un acuerdo de voluntades, como cualquier contrato tradicional; que debe ser necesariamente entre personas distantes, lo que implica un tratamiento singular no coincidente con la definición doctrinal; y la necesidad de que la oferta y la aceptación deban ser manifestadas por medios electrónicos. Por todo ello, puede concluirse que la definición que se recoge en la normativa española sobre contrato o contratación electrónica es más restrictiva que las directrices comunes consideradas por la doctrina, *ad supra*. Sin embargo, se ha ampliado la aplicabilidad de la Ley a más instrumentos electrónicos de los primitivamente regulados[77].

[76] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758. Último acceso: 08.08.2018.

[77] El apartado 6.º de la letra a) del anexo fue derogado por el apartado 18 de la disposición derogatoria de la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual. En este se recogía:
"No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:
1.º Los servicios prestados por medio de telefonía vocal, fax o télex.
2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.
..."

Para finalizar este análisis, por su carácter internacional y su poder uniformador, no podemos obviar que La Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (1996)[78] tiene como ámbito de aplicación "*todo tipo de información en forma de mensaje de datos utilizada en el contexto de actividades comerciales"* (artículo 1), expandiendo el término comercial a "*las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual"*.[79]

Diseccionado el concepto de contratación electrónica en el elenco jurídico que regula, de una forma genérica o específica, este nuevo proceso de contratación, estamos en condiciones de delimitar términos intrínsecamente relacionados.

Analizado en el primer apartado qué debe entenderse por contratos informáticos, el siguiente paso es analizar si ese instrumento jurídico supone un modelo típico y propio. La mayoría de la doctrina es clara al respecto, los contratos informáticos se regirán por las disposiciones generales de los contratos, por lo tanto, debemos atender a las normas establecidas en el Código civil, dependiendo de los sujetos intervinientes y los objetos del contrato, a las normas que se dictan en el Código de comercio, si puede calificarse como acto de comercio, a la normativa referente a la protección de los consumidores y usuarios, o a las prerrogativas de la contratación pública y los contratos administrativos. DÁVARA RODRÍGUEZ[80], siguiendo la línea anteriormente expuesta, recoge *"*(los contratos informáticos) *los tenemos que encuadrar en la teoría general de los contratos"*, complementando MADRID PARRA[81] que, entre las especialidades de los contratos informáticos, se encuentra su atipicidad, de tal forma que se configura sobre *"la base del principio de autonomía de la voluntad y, en buena medida, con aplicación del régimen*

[78] Accesible en: http://daccess-ods.un.org/access.nsf/Get?Open&JN=N9776360 y https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf. Último acceso: 08.08.2018.

[79] En el próximo apartado, "Principios comunes y específicos en el marco del comercio electrónico", se abordará las implicaciones de la Ley Modelo sobre Comercio Electrónico. Para no ser reiterativos, emplazamos su estudio, salvo con las breves notas esenciales para la reflexión del presente, al próximo punto de análisis.

[80] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi, p. 264.

[81] MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 78.

jurídico de los contratos de arrendamientos de obra o de servicios". En conclusión, podemos hacer nuestras las palabras de MÚGICA ARRIEN[82], que tras refrendar la atipicidad de los contratos informáticos y la imposibilidad de establecer un modelo único de contrato informático, expone que *"no están regulados de forma específica. Esto nos lleva a acudir a la teoría general de la contratación, sin obviar, claro está, que estos contratos tienen una serie de características y circunstancias propias"*.

Tanto la contratación electrónica[83] como los contratos informáticos pueden desarrollarse a través de canales en los que sujetos intervinientes se encuentran ausentes, de ahí que sea aplicable la regulación de los contratos entre ausentes. MENÉNDEZ MATO[84] afirma que permite agilizar la conclusión (los medios electrónicos, y en especial Internet) de contratos entre partes físicamente no presentes gracias a la celeridad del sistema.

Antes de citar la normativa al respecto, y a tenor del artículo 1.262 del Código civil y el artículo 54 del Código de comercio, es necesario tener presente que la concepción de contrato a distancia adquiere un significado más amplio cuando se trata de consumidores, no solo por la normativa posterior que se desarrolla sino por su propio contenido. Contrato a distancia no es sinónimo de contrato entre ausentes.

El contrato a distancia ha sido definido como la transmisión de la aceptación contractual, al menos, de partes que no están físicamente presentes. Sin embargo, el contrato entre ausentes restringe su ámbito de aplicación a los contratos, no siendo aplicable a la contratación entre personas que estén físicamente distantes pero que empleen un medio técnico que les permita la comunicación a distancia. Es sabido que lo que caracteriza al contrato entre ausentes es que la aceptación de las partes se realice en ausencia de los intervinientes, siendo irrelevante a efectos de aplicabilidad cualquier momento anterior. La evolución de la técnica ha determinado una característica, en la

[82] MÚGICA ARRIEN, Gotzone: "Los contratos informáticos", *SABERES, revista de estudios jurídicos, económicos y sociales*, 2003, Universidad Alfonso X El Sabio, Vol. 1, pag. 2. Accesible en: https://revistas.uax.es/index.php/saberes/article/view/687. Último acceso: 08.08.2018.

[83] Ad *supra* se ha reseñado como algunos autores, entre ellos ILLESCAS ORTIZ, considera que el comercio electrónico siempre se desarrolla entre ausentes.

[84] MENÉNDEZ MATO, Juan Carlos: "Perspectiva espacio-temporal: La conclusión del contrato desde Internet", *El contrato vía Internet*, 2005, J.M. Bosch editor, p. 279.

mayoría de las relaciones contractuales, que lo diferencia de la tradicional contratación entre ausentes, lo que MORENO NAVARRETE[85] ha denominado *"contratación entre ausentes en tiempo real"*. Más correcto hubiera sido indicar, dado que son categorías jurídicas distintas, que es común encontrarnos con contratos entre sujetos presentes, pero, y a su vez, contratos a distancia cuando uno de los sujetos intervinientes sea un consumidor. Sin entrar en una disertación teórica al respecto, que podría difuminar el estudio del presente capítulo, podríamos encontrarnos con contratos de formación instantáneas, gracias a los nuevos medios electrónicos que permiten la comunicación instantánea con un intercambio inmediato de la oferta y su aceptación, y ser considerados "a distancia" por la presencia de un consumidor y tratarse de una relación sin presencia física de las partes.

La Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores[86] define en su artículo 2.7) el contrato a distancia como aquel que se produce sin la presencia física simultánea de las partes utilizando una o más técnicas de comunicación a distancia hasta la celebración o en la celebración, si bien, lo limita al ámbito de aplicación de la ley, contrato celebrado entre comerciante y consumidor. La Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, antes mencionada, define de forma más escueta qué se entiende por "a distancia", aunque no directamente relacionado con la contratación sino con el posible objeto de la misma, en este supuesto, servicios de la sociedad de la información. En este sentido, considera que es un servicio prestado sin que las partes estén presentes simultáneamente. Sin embargo, lo realmente relevante es, a los efectos de nuestro actual estudio, qué considera servicios no ofrecidos a distancia y no ofrecidos por vía electrónica. En el primero de los casos, aunque se utilicen medios electrónicos, no se considerará a distancia cuando el servicio se realice en presencia física del prestador y destinatario; y en el segundo supuesto, limita los dispositivos electrónicos afectos a la consideración de "vía electrónica".

[85] MORENO NAVARRETE, Miguel Ángel: "Los fundamentos del contrato electrónico", *DERECHO-e Derecho del Comercio electrónico*, 2002, Marcial Pons, p. 47.

[86] Accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2011-82312. Último acceso: 08.08.2018.

En el marco español, la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista[87] se ocupa de las "ventas a distancia". Sin embargo, tras las diferentes disposiciones posteriores, el único artículo que no ha quedado derogado referente a la venta a distancia es el artículo 39, que delimita el objeto remitiéndose al Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias[88]. Esta disposición define la venta a distancia como los contratos celebrados *"con los consumidores y usuarios en el marco de un sistema organizado de venta o prestación de servicios a distancia, sin la presencia física simultánea del empresario y del consumidor y usuario, y en el que se hayan utilizado exclusivamente una o más técnicas de comunicación a distancia hasta el momento de la celebración del contrato y en la propia celebración del mismo".* Curiosamente, el artículo 94 del citado texto, referente a los contratos celebrados a distancia y los contratos celebrados fuera del establecimiento mercantil, determina cómo los contratos electrónicos son una modalidad de contratación a distancia, estableciendo que su regulación será aplicable a los mismos[89].

Delimitados conceptualmente los términos afectos, es necesario determinar las notas o principios básicos.

d. Principios comunes y específicos en el marco del comercio electrónico

Ad supra, cuando hemos estudiado la delimitación de los conceptos de contratación informática y contratación electrónica, en el marco de las definiciones recogidas en la normativa existente, se ha reseñado brevemente la Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. En el estudio de los principios y estándares básicos del comercio electrónico, y por ende de los contratos por medios electrónicos, será marco de referencia

[87] Accesible en: http://www.boe.es/buscar/act.php?id=BOE-A-1996-1072. Último acceso: 08.08.2018.

[88] Accesible en: http://www.boe.es/buscar/act.php?id=BOE-A-2007-20555. Último acceso: 08.08.2018.

[89] En concreto establece: "*en las comunicaciones comerciales por correo electrónico u otros medios de comunicación electrónica y en la contratación a distancia de bienes o servicios por medios electrónicos, se aplicará además de lo dispuesto en este título, la normativa específica sobre servicios de la sociedad de la información y comercio electrónico"*. Añadiendo en su párrafo segundo: "c*uando lo dispuesto en este título entre en contradicción con el contenido de la normativa específica* (contratos a distancia o fuera del establecimiento mercantil) *sobre servicios de la sociedad de la información y comercio electrónico, esta será de aplicación preferente, salvo lo previsto en el artículo 97.7, párrafo segundo".*

y apoyo en pos de favorecer la confianza entre las partes, primar la autonomía de la voluntad privada, la transparencia, la rapidez y el equilibrio cuando se emplee los medios electrónicos en los contratos, en la búsqueda de garantizar de la legalidad.

La Ley Modelo sobre Comercio Electrónico nace con una doble finalidad[90]:

- Servir de respuesta a los ciudadanos ante los nuevos medios de comunicación utilizados para sus relaciones de negocios.
- Como texto normativo de apoyo para actualizar la normativa legal y la práctica de los Estados en materia contractual y de negocios ante el empleo de nuevos medios (electrónicos).

Se intenta crear, por tanto, un conjunto de reglas jurídicas uniformes con el fin de salvaguardar las incertidumbres jurídicas que suscitaba el empleo de los medios electrónicos de comunicación, sobre todo ante las posibles contradicciones o lagunas que pudieran subsistir en las disposiciones legislativas de los distintos Estados[91].

Los principios básicos que nos marcan las Leyes Modelo, principalmente la de Comercio electrónico, tienen carácter trasversal, determinando normas de carácter horizontal y generales aplicables a todos los contratos electrónicos o realizados a través de medios electrónicos[92]. La Ley Modelo no supone un Derecho objetivo directamente aplicable, sin embargo, articula una guía para que de forma armonizada se pueda normativizar en la materia. Tanto es así, como hemos apreciado, que ha sido el marco de referencia en diferentes disposiciones posteriores, entre otras la Directiva 2000/31/CE de Comercio Electrónico y la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico.

---

[90] MORENO NAVARRETE, Miguel Ángel: "Los fundamentos del contrato electrónico", *DERECHO-e Derecho del Comercio electrónico*, 2002, Marcial Pons, p. 11.

[91] Expresamente, en la Resolución aprobada por la Asamblea General sobre la base del informe de la Sexta Comisión A/51/628, recoge: *"estimando que la aprobación de la Ley Modelo sobre Comercio Electrónico por la Comisión ayudará de manera significativa a todos los Estados a fortalecer la legislación que rige el uso de métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel y a preparar tal legislación en los casos en que carezcan de ella"*. Accesible en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf. Último acceso: 08.08.2018.

[92] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 10-11 y 18-19.

En materia contractual es sustancial acudir al principio de la buena fe como base de las relaciones entre partes, por la cual cada uno de los intervinientes cumplirá con las relaciones jurídicas manifestadas, consumando lo pactado. La confianza mutua en los predisponentes permite el empleo de nuevos medios por el que canalizar las relaciones contractuales, que avanzan más rápidamente que la regulación a las que estarán afectos. De otra forma, en primer lugar, tendríamos que esperar a regular de forma particularizada cada una de las novedades que se plantean en las denominadas nuevas tecnologías, y por otra, como pone de manifiesto MADRID PARRA[93], estaríamos elaborando un Derecho y una tecnología con una finalidad, principalmente, para impedir el fraude, el engaño o el incumplimiento contractual de las partes, pretendiendo que la esfera privada del Derecho, como es el contractual, ejerza un papel propio del Derecho público, en concreto, del Derecho penal. Por lo tanto, y aunque posteriormente se estudiará con detenimiento como principio específico del Derecho del comercio electrónico, es una manifestación más de la inalterabilidad del derecho preexistente en las obligaciones contraídas entre las partes.

A pesar de ser un principio general del Derecho de contratos, la Ley Modelo sobre Comercio Electrónico no se resiste a recogerlo como fundamento principal de los contratos por medios electrónicos. El artículo 3.1 reconoce "*en la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe"*, al igual que establece el artículo 57[94] del Código de comercio. En conclusión, el principio de la buena fe contractual acontece esencial en la contratación por medios electrónicos porque, como afirma ILLESCAS ORTIZ[95], muchos de los usuarios y sus consejeros jurídicos no conocen certeramente el empleo de esta nueva tecnología, siendo en algunos casos mediada por expertos en la materia, por lo que requiere mayor firmeza y rigor la afirmación de la buena fe contractual.

---

[93] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 20.

[94] Artículo 57 del CCo: "*Los contratos de comercio se ejecutarán y cumplirán de buena fe, según los términos en que fueren hechos y redactados, sin tergiversar con interpretaciones arbitrarias el sentido recto, propio y usual de las palabras dichas o escritas, ni restringir los efectos que naturalmente se deriven del modo con que los contratantes hubieren explicado su voluntad y contraído sus obligaciones"*.

[95] ILLESCAS ORTIZ, Rafael: "Los principios generales del Derecho del comercio electrónico", *Derecho de la Contratación Electrónica,* 2009, Civitas, p. 58.

En el Derecho contractual se establece como uno de los principios esenciales el principio de autonomía de la voluntad[96]. Cuando se habla de autonomía de la voluntad se incide no solo en la voluntad de los contrayentes en someterse a una relación contractual, sino a la libertad de dotar de contenido y de regir la relación contractual dentro del ámbito de libertad de las partes. En el ámbito de contratos, se encuentra establecido en nuestro Código civil en el artículo 1.255[97], y aparece también, aunque de forma difusa, en el artículo 11.1 de la Ley Modelo sobre Comercio Electrónico al recogerse que *"...de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos"*. Por lo tanto, el poder de voluntad de las partes se configura como principio vertebrador y esencial, también, en la contratación electrónica.

La incidencia directa es que no es necesario un reconocimiento o, dicho de otro modo, norma habilitante para el empleo de los medios electrónicos en la contratación a través de estos instrumentos, siendo vinculante para las partes. Como contrapeso, este principio, además de habilitar el empleo de los medios electrónicos para contratar, limita la posibilidad de anteponer el empleo de los medios electrónicos a la voluntad de los intervinientes en el contrato. Por lo tanto, la normativización del empleo de los medios electrónicos en la contratación da certidumbre a los efectos jurídicos que producen por el principio citado, pero deben ser las partes las que delimiten su actuación. Como bien indica MADRID PARRA[98], *"la existencia de normas relativas a la contratación electrónica ni amplia ni aminora el ámbito de actuación del que disponen las partes. Será el Derecho sustantivo aplicable a cada contrato el que determine los límites al ámbito de actuación de las partes"*. De esta forma, en el marco del comercio electrónico, y por tanto

[96] En el ámbito de la resolución electrónica de conflictos, VILALTA NICUESA hace hincapié en que el alcance resultará distinto según nos encontremos en un sistema autocompositivo o adversarial. VILALTA NICUESA, Aura Esther: "Resolución electrónica de conflictos", *Principios de Derecho de la Sociedad de la Información*, 2010, Aranzadi- Thomson Reuters, p. 331.

[97] Dicta así: *"los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público.*

[98] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 19.

de la contratación electrónica, el principio de autonomía de voluntad puede ser un instrumento que impulse este espacio de comunicación[99].

Define DÍEZ-PICAZO[100] la forma del contrato como *"aquello que pueda servir de vehículo a su exteriorización* (la voluntad individual) *y, por tanto, todos los contratos son formales, pues todos necesitan de alguna forma para celebrarse y aparecer en Derecho*". Sin embargo, el propio DÍEZ-PICAZO matiza que, cuando se discute o analiza la forma del contrato hacemos referencia al requisito necesario de una forma de exteriorización para la válida constitución del contrato, bien sea impuesta por las partes o por ley[101].

El principio de libertad de forma, aunque con autonomía propia, está estrechamente vinculado al principio de autonomía de la voluntad de las partes. Como señala DE MIGUEL ASENSIO[102], en el ámbito electrónico el cumplimiento del requisito de forma en los contratos puede presentar dificultades, al asociarse con el empleo del soporte papel. Las partes, por consecuencia del citado principio, quedan obligadas en cualquiera de las formas que determinen los intervinientes. Será, por tanto, la excepción imponer una forma a la hora de contratar. De este modo, el principio de equivalencia funcional refuerza el empleo de libertad de forma, con incidencia directa para determinar cuándo y cómo se ha documentado correctamente un escrito, su valoración como medio de prueba o cuándo se han cumplido los requisitos de forma exigidos para la validez del contrato. En consecuencia, se refuerza el argumento anteriormente expuesto de que las partes pueden seleccionar los medios electrónicos como instrumentos para perfeccionar contratos. En España, el principio de libertad de forma se encuentra reconocido en el artículo 1.278[103]

---

[99] LÓPEZ JIMÉNEZ, David: "Consideraciones de carácter general relativas al comercio electrónico: vino nuevo sobre odres viejos", *Nuevas coordenadas para el Derecho de obligaciones. La autodisciplina del comercio electrónico*, 2013, Marcial Pons, p. 30.

[100] DÍEZ-PICAZO Y PONCE DE LEÓN, Luis: "La forma y la documentación del contrato", *Fundamentos del Derecho Civil Patrimonial*, 2012, Civitas, Vol.I, p. 287.

[101] DÍEZ-PICAZO Y PONCE DE LEÓN, Luis: "La forma y la documentación del contrato", *Fundamentos del Derecho Civil Patrimonial*, 2012, Civitas, Vol.I, p. 287.

[102] DE MIGUEL ASENSIO, Pedro Alberto: "Contratación electrónica", *Derecho Privado de Internet*, 2011, Civitas-Thomson Reuters, p. 833.

[103] Artículo 1.278 del CC: *"Los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez"*.

del Código civil y en el artículo 51[104] del Código de comercio, por lo tanto, la eficacia obligatoria y validez del contrato, tras la concurrencia de la oferta y la aceptación (artículo 1.262[105] del Código civil), se encuentran debidamente reconocidas antes de cualquier introducción o novedad normativa relativa a la validez del empleo de los medios electrónicos.

A lo largo de toda la disertación se ha hecho patente que el empleo de los nuevos medios electrónicos, y los que están por venir, afectan al ordenamiento jurídico en su conjunto, por lo tanto, sería temerario pensar en una revisión de todo el Derecho que se ve influenciado por las nuevas tecnologías. Como salvaguarda, se formula el principio de inalterabilidad del Derecho preexistente. Respetando el régimen jurídico preexistente se formularán normas de carácter general, que podemos determinar básicas, para regular el empleo del medio electrónico, no pretendiendo una regulación específica[106]. Por lo tanto, y en palabras de ILLESCAS ORTIZ[107], *"*(se) *parte de la hipótesis conforme a la cual la electrónica no es sino un nuevo soporte y medio de transmisión de voluntades negociales pero no un nuevo derecho regulador de las mismas y su significación jurídica"*. Sin embargo, como argumenta MADRID PARRA[108], la evolución de la regulación de las nuevas tecnologías ha propiciado, en primer lugar, el empleo de normas específicas que sí han alterado el Derecho preexistente, y en otro orden, el legislador tiene presente el

[104] Artículo 51 del CCo: *"Serán válidos y producirán obligación y acción en juicio los contratos mercantiles, cualesquiera que sean la forma y el idioma en que se celebren, la clase a que correspondan y la cantidad que tengan por objeto, con tal que conste su existencia por alguno de los medios que el Derecho civil tenga establecidos…"*.

[105] El citado artículo fue modificado por la Ley 34/2002, de 11 de julio (LSSICE). Antes de la reforma del 12 de octubre de 2002, se omitía cualquier referencia a los medios electrónicos, estando redactado*: "El consentimiento se manifiesta por el concurso de la oferta y la aceptación sobre la cosa y la causa que han de constituir el contrato.*
La aceptación hecha por carta no obliga al que hizo la oferta sino desde que llegó a su conocimiento. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta".

[106] Su plasmación normativa la podemos apreciar, por ejemplo, en el artículo 23.1 de la LSSICE, que al regular la validez y eficacia de los contratos celebrados por vía electrónica promulga que *"los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial"*.

[107] ILLESCAS ORTIZ, Rafael: "Los principios generales del Derecho del comercio electrónico", *Derecho de la Contratación Electrónica,* 2009, Civitas, p. 49.

[108] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 25-26.

fenómeno tecnológico en la nueva regulación. En consecuencia, aunque la inalterabilidad del Derecho preexistente es efectiva y general, no está teniendo proyección en la regulación jurídica actual, al ser cada vez más recurrente emplear principios propios de las nuevas tecnologías en el marco normativo, conformando un cuerpo reglamentario propio[109].

DE MIGUEL ASENSIO[110] ya manifestaba que es imprescindible, para el desarrollo de la contratación por medios electrónicos, que el ordenamiento jurídico reconozca efectos jurídicos equiparables a las declaraciones de voluntad manifestadas por los soportes tradicionales. El principio de equivalencia funcional es propio de la regulación del comercio electrónico y, por ende, de la contratación electrónica. ILLESCAS ORTIZ[111], dentro del ámbito de actuación de este principio, incluye la no discriminación de los contratos celebrados, en nuestro estudio, por medios electrónicos. Es decir, engloba la vertiente positiva y negativa de la formulación en un solo principio.

Optando por estudiar por separado los principios implicados, como disecciona MADRID PARRA[112], el principio de no discriminación implica que no puede excluirse la aplicabilidad, consentimiento, perfección y, en general, el régimen jurídico contenido en los contratos celebrados por medios electrónicos por razón del empleo del propio medio. Su promulgación en los textos normativos es más evidente y diferenciada que el principio de equivalencia funcional, con las siguientes reseñas: en la Ley Modelo sobre Comercio Electrónico, el artículo 11.1 manifiesta, en referencia a la formación y validez de los contratos, que "*no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos"* y el artículo 12.1 recoge, en referencia al reconocimiento por las partes de los mensajes de datos, que "*no*

[109] Un claro ejemplo nos lo encontramos con la banca en línea, y la regulación de los fraudes relativos a su empleo como el *phishing, el pharming o spam*. Tomando, por ejemplo, el supuesto del *spam*, su regulación se encuentra recogida en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico en los artículos 19, 20, 21, 22, 38 y 43 y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones en sus artículos 38, 53.z, 54.r, 58.b y D.A. Novena.

[110] DE MIGUEL ASENSIO, Pedro Alberto: "Contratación electrónica", *Derecho Privado de Internet*, 2011, Civitas-Thomson Reuters, p. 831.

[111] ILLESCAS ORTIZ, Rafael: "Los principios generales del Derecho del comercio electrónico", *Derecho de la Contratación Electrónica,* 2009, Civitas, p. 39-49.

[112] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 20-24.

se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos". En el Derecho patrio, la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico recoge el citado el principio en el artículo 23, en referencia a la validez y eficacia de los contratos celebrados por vía electrónica, al mostrar que *"los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico"* y *"para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos"*. Por lo tanto, a pesar de la inmaterialidad del medio, en comparación con la percepción directa del soporte papel, deben ser considerados con iguales efectos jurídicos. En este sentido, MORENO NAVARRETE[113] reitera que el principal problema del documento electrónico es su intangibilidad, argumentando que es oportuna su incorporación en un medio tangible para que cumpla idéntico fin que el papel. Como posteriormente veremos al tratar el principio de equivalencia funcional, esta necesaria corporeidad será requisito *sine qua non* para asimilar el escrito digital y el original digital a sus semejantes en soporte papel.

La vertiente positiva del principio de no discriminación se manifiesta tras el principio de equivalencia funcional. Supone que los medios electrónicos pueden cumplir las mismas funciones que los distintos ordenamientos jurídicos hacen recaer en los medios tradicionales, sin entrar a modificar el Derecho sustantivo contractual, en particular en cuanto a la exigencia del escrito, firma u original. Para vislumbrar la manifestación del principio en la Ley Modelo sobre Comercio Electrónico, tenemos que acudir al artículo 6[114], titulado escrito, artículo 7[115], firma, y artículo 8[116], original. Siempre que posibilite la consulta, pueda identificar a la persona y vincularla con la información del mensaje electrónico, y se conserve la integridad de la información desde su forma definitiva de

[113] MORENO NAVARRETE, Miguel Ángel: "Los fundamentos del contrato electrónico", *DERECHO-e Derecho del Comercio electrónico*, 2002, Marcial Pons, p. 38-39.

[114] Artículo 6.1 de la LMCE: *"Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que este contiene es accesible para su ulterior consulta."*.

[115] El artículo 7.1 de la LMCE recoge: *"cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos…"*.

[116] El artículo 8.1 de la LCME estable: *"cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos…"*.

creación, según los casos, el soporte electrónico, según la Ley Modelo, es equivalente al soporte papel. Más claro se manifiesta el principio en la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, Título IV, cuando trata la "contratación por vía electrónica". Tras reconocer en el apartado 1 del artículo 23 que producirán todos los efectos previstos en el ordenamiento jurídico los contratos celebrados por vía electrónica, es el apartado 3 el que explicita el principio de equivalencia funcional al aprobar "*siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico"*, así como el artículo 24.2[117] determina *"en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental"*. Por consiguiente, al igual que la Ley Modelo, establece el principio de equivalencia funcional para los escritos y su función como medio de prueba. MADRID PARRA[118] argumenta que el principio de equivalencia funcional recogido en el artículo 23.3, aunque directamente regula el escrito, tiene mayor transcendencia, apunta a valor jurídico de toda la información que conste en soporte electrónico. Debemos añadir que, siguiendo a DE MIGUEL ASENSIO[119], la equivalencia funcional resulta no solo de la celebración del contrato sino de todos los deberes relativos a la entrega en forma escrita, la formación del contrato, el cumplimiento del contrato y las consecuencias administrativas derivadas.

En resumen, y tratando, ahora sí, de forma conjunta los principios de no discriminación y de equivalencia funcional, podemos decir que el documento electrónico y el empleo de

[117] En el supuesto de la firma electrónica podemos ver la casuística que nos encontramos al tratar el principio de equivalencia funcional. El artículo 3.4 de la Ley 59/2003, de 19 de diciembre, de firma electrónica establece *"la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel"*. Sin embargo, debe coligarse con el principio de no discriminación y cómo a pesar de su promulgación en el artículo 3.9, solo la firma electrónica reconocida tiene la efectiva equivalencia. Para saber más sobre la neutralidad tecnológica de la firma electrónica y equivalencia funcional de la firma electrónica, vid. MADRID PARRA, Agustín: "Tramitación y contenido de la Ley Modelo de la CNUDMI/UNCITRAL sobre las firmas electrónicas", *El contrato por medios electrónicos*, 2003, Universidad Externado de Colombia, p. 1591 y MADRID PARRA, Agustín: "Aspectos jurídicos de la identificación en el comercio electrónico", *Derecho del comercio electrónico*, 2001, p. 211.

[118] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 23.

[119] DE MIGUEL ASENSIO, Pedro Alberto: "Contratación electrónica", *Derecho Privado de Internet*, 2011, Civitas-Thomson Reuters, p. 835.

los medios electrónicos para la contratación son soportes e instrumentos suficientes para la exteriorización de la voluntad de los contratantes, semejante al documento material, o en sentido estricto, el papel. Como podemos apreciar, la regulación nace de las exigencias expuestas en el artículo 9 de la Directiva sobre el comercio electrónico[120]. Sin embargo, a pesar de los esfuerzos, cuando sea requerida la forma *ad solemnitaten* en la formalización de los negocios jurídicos no podrá canalizarse la manifestación de la voluntad por medios e instrumentos electrónicos.

Uno de los problemas que nos encontramos cuando los medios electrónicos intervienen en el negocio jurídico, y por tanto en la contratación, es que una regulación del fenómeno contractual, que siempre llega tarde, puede discriminar entre los medios electrónicos existentes y las evoluciones futuras de los medios de intercambio, principalmente por el desconocimiento de los sistemas electrónicos que han de venir. Esta discriminación no solo mermaría la confianza en el empleo de los medios electrónico de los usuarios, sino que retrasaría de forma significativa la evolución de estas herramientas, que puede tener incidencias, entre otros aspectos, en la seguridad o rapidez de los medios. Este argumento, que ya justifica la aparición del principio de equivalencia funcional y no discriminación, es la razón de ser del principio conocido como neutralidad en el uso de la tecnología o neutralidad normativa en relación con la tecnología. Se tiende a respetar el efecto jurídico independientemente del empleo de una tecnología frente a otra. En palabras del MADRID PARRA[121], se pretende formular un entorno jurídico neutro, apoyado en la no discriminación de ninguna de las técnicas que pudieran utilizarse para comunicarse o archivar información. En consecuencia, la norma jurídica que regula el empleo de los medios electrónicos no puede discriminar, de forma positiva o negativa, por la tecnología empleada.

En el seno de la contratación electrónica ninguna norma jurídica pregona el principio ahora expuesto, si bien, sí puede vislumbrarse en la Guía para la incorporación de la Ley

[120] El artículo 9.1 de la DCE: *"1. Los Estados miembros velarán por que su legislación permita la celebración de contratos por vía electrónica. Los Estados miembros garantizarán en particular que el régimen jurídico aplicable al proceso contractual no entorpezca la utilización real de los contratos por vía electrónica, ni conduzca a privar de efecto y de validez jurídica a este tipo de contratos en razón de su celebración por vía electrónica".*

[121] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 24-25.

Modelo sobre el Comercio Electrónico[122]. El punto 6, dentro del apartado "objetivos", recomienda que *"al incorporar a su derecho interno los procedimientos prescritos por la Ley Modelo para todo supuesto en el que las partes opten por emplear medios electrónicos de comunicación, un Estado estará creando un entorno legal neutro para todo medio técnicamente viable de comunicación comercial"*, reforzado con el contenido establecido en el punto 8, dentro del "ámbito de aplicación", al predicar que "*responde así a la necesidad en que se encuentran los usuarios del comercio electrónico de poder contar con un régimen coherente que sea aplicable a las diversas técnicas de comunicación que cabe utilizar indistintamente. Cabe señalar que, en principio, no se excluye ninguna técnica de comunicación del ámbito de la Ley Modelo, que debe acoger en su régimen toda eventual innovación técnica en este campo"*[123]. Tal es la importancia del principio de neutralidad tecnológica que en la nota explicativa de la Secretaría de la CNUDMI de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[124] se recoge como "principio primordial", junto con el de equivalencia funcional, guiando toda la labor de la CNUDMI en materia de comercio electrónico[125].

e. En relación con el contrato del *cloud computing*

En el Capítulo I definíamos el concepto de la computación en la nube o *cloud computing*. De manera resumida podemos tomar el esquema expuesto por GARCÍA DEL

---

[122] Accesible, junto a la Ley Modelo sobre el Comercio Electrónico, en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf. Último acceso: 08.08.2018.

[123] Este principio sí se encuentra recogido en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas en su artículo 3, a pesar de que claramente discrimina sobre algunos tipos de firmas electrónicas. Accesible en: http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf. Último acceso: 08.08.2018. En sintonía, MORENO NAVARRETE considera que es la firma electrónica la principal figura sobre la que versa el principio de neutralidad tecnológica (MORENO NAVARRETE, Miguel Ángel: "Los fundamentos del contrato electrónico", *DERECHO-e Derecho del Comercio electrónico*, 2002, Marcial Pons, p. 154-156).

[124] Accesible en: https://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf. Último acceso: 08.08.2018. En la propia nota se recoge que *"la neutralidad tecnológica es particularmente importante habida cuenta de la velocidad de la innovación y del desarrollo tecnológicos, y contribuye a asegurar que la ley dará cabida a las futuras novedades tecnológicas y evitar que caiga rápidamente en desuso"* (párrafo 48, p. 29).

[125] Aunque no es objeto directo de nuestro estudio, no podemos obviar que la aplicabilidad del principio de neutralidad tecnológica ha tenido difícil soporte en la regulación de la firma electrónica. Véase los distintos efectos probatorios que la Ley de Firma Electrónica establece para la firma electrónica reconocida, avanzada y sencilla.

POYO VIZCAYA[126], independientemente del modelo de implantación, esta tecnología permite almacenar la información de manera permanente en distintos servidores a través de los cuales los usuarios pueden recuperar la información mediante Internet cuando así lo requieran, remitiéndose directamente a sus dispositivos siguiendo una serie de procedimientos preestablecidos. Dentro de estos servicios de la nube, los contratos pueden clasificarse según el modelo de implementación en 4 categorías: procesamiento corriente de textos y servicios de correo; hospedaje de datos; utilización de programas informáticos o bases de datos bajo licencias y otros derechos de propiedad intelectual protegidos; y productos de trabajo de propiedad exclusiva[127].

Con independencia del carácter contractual, según las partes contratantes, que se delimitará en capítulos posteriores, nos enfrentamos a un contrato de prestación de servicios informáticos que requiere la externalización[128]. Por tanto, debemos partir en primer lugar de la definición de externalización de servicios que, aunque parezca baladí, ayudará a delimitar este servicio informático. DÁVARA RODRÍGUEZ[129] conceptualiza el *outsourcing* informático como *"la cesión de la gestión de los sistemas de información de una entidad por un tercero que, especializado en esta área, se integra en la toma de decisiones y desarrollo de las aplicaciones y actividades propias de la referida gestión, la finalidad de la optimización de los resultados"*, basado en el empleo de las nuevas tecnologías y la especialización de la tecnología del tercero. El problema que se plantea con la vinculación del contrato de la computación en la nube y la definición presentada por DÁVARA RODRÍGUEZ sobre la externalización informática es el alcance en la gestión del tercero, sobre todo en el modelo de implantación *IaaS*. Si bien, como ya estableciéramos *ad supra*, la mayoría de los servicios que se ofrecen en la nube como

[126] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing", *Derecho y Cloud computing*, 2012, Thomson Reuters, p. 178.

[127] CNUDMI: "Posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube" - Propuesta del Gobierno del Canadá" 48º Período de sesiones, 2015, p. 16. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V15/040/53/PDF/V1504053.pdf. Último acceso: 08.08.2018.

[128] Similar consideración ha manifestado MADRID en el estudio de los contratos informáticos por razón del objeto (MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 78).

[129] DÁVARA RODRÍGUEZ, Miguel Ángel: "El comercio electrónico y la contratación electrónica", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi, p. 278.

"almacenamiento" enmascaran una estructura *SaaS*, teniendo el proveedor de servicios cada vez más un papel relevante. Añade ROSELLÓ RUBERT, como diferencia entre el contrato tradicional de *outsourcing* y la nube, la posibilidad de compartir el entorno entre diferentes clientes, no previsto para el *outsourcing*, posibilitando el uso a clientes sin necesidad de conocimientos técnicos elevados[130]. No hay que perder de vista que una de las razones para la implantación del *cloud* es la reducción en costes estructurales y la optimización de los recursos propios de la empresa. ALARCÓN FIDALGO[131] nos recuerda que las prestaciones más típicas del contrato del *cloud computing* son, en primer lugar, el almacenamiento en la nube, clasificándose los contratos reguladores por algunos autores como arrendamientos de servicios, arrendamiento de obra o contrato de depósito; y, en segundo lugar, de suministro de aplicaciones, donde el proveedor en la mayoría de las ocasiones ni las desarrolla ni las programa, sino que las obtiene de otro productor o programador ajeno a la relación contractual, con la complejidad de contratos relacionados con los servicios.

El contrato del *cloud computing* tiene una naturaleza compleja y atípica que se regirá, como en posteriores capítulos tendremos la oportunidad de ver, por los Acuerdos de Niveles de Servicios (ANS o SLA) que se determinarán en las cláusulas contractuales particulares o Anexos al contrato principal. Sin embargo, esa atipicidad que ahora predicamos de la contratación de la nube no debe ser considerada como radical, como establece APARICIO VAQUERO[132]. El carácter atípico viene marcado por la complejidad del contrato, al mezclarse dos tipos contractuales: los contratos de obras y de servicios. Esta configuración provocará que nos enfrentemos, al analizar los contratos del *cloud*, a cláusulas de prestaciones de medios y a cláusulas de prestaciones de resultados. Estas obligaciones de medios y de resultado devienen esenciales para la correcta ejecución del objeto, determinando la responsabilidad de las partes en caso de incumplimiento. La parte contratante de la nube delega en el prestador de servicios

[130] ROSSELLÓ RUBERT, Francisca María: "Concepto y características técnicas del *Cloud Computing*", *Cloud Computing. Régimen Jurídico para Empresarios*, 2018, Thomson Reuters Aranzadi, p. 46-47.

[131] ALARCÓN FIDALGO, Joaquín: "Cloud computing, responsabilidad y seguro", *Revista española de seguros: Publicación doctrinal de Derecho y Economía de los Seguros privados*, 2013, núm. 153-154, p. 35.

[132] APARICIO VAQUERO, Juan Pablo: "Elementos y naturaleza de la relación de *outsourcing*", *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 2002, Comares, p. 72.

funcionalidades propias, dadas las características del objeto contractual, lo que conlleva establecer una serie de compromisos, aunque continuamente se haya catalogado el contrato como prestación de servicios, siendo el estándar de este tipo de contratos generar obligaciones de medios y no de resultados.

En conclusión, siempre que el contrato de la nube respete los preceptos contenidos en el artículo 1.255 del Código civil y existiendo consentimiento, objeto y causa, artículo 1.261 del Código Civil, la regulación se regirá por lo pactado por las partes, artículo 1.091 del Código Civil, bajo los principios y los usos generales y específicos en material contractual anteriormente establecidos. Es claro, por tanto, que el contrato del *cloud* es un contrato informático en razón de su objeto, y comúnmente, electrónico por razón del medio a través del cual se contrata.

CAPÍTULO III - INICIATIVAS LEGALES. **a. Anteproyecto de Ley de Código Mercantil Español**: *a. Introducción. Principios comunes y específicos en el marco del comercio electrónico. b. Tipificación de los contratos de comunicaciones electrónicas: i. Contrato de servicios de comunicación electrónica, ii. Contrato de alojamiento; iii. Acuerdos para la copia temporal de datos o información. c. Incidencia del Anteproyecto de Ley de Código Mercantil en la contratación del cloud computing*. **b. Actividad de Grupo Europeo de Protección de Datos "artículo 29"**: *a. Introducción: qué es el Grupo de Trabajo del artículo 29 y contexto en la prestación del servicio del cloud computing. b. Recomendaciones del Grupo de Trabajo del artículo 29 para la prestación del servicio del cloud computing..* **c. Experiencias internacionales**. **d. Principios comunes y específicos en el marco del comercio electrónico**. **e. En relación con el contrato del *cloud computing*:** *a. Primeros pasos: FedRAMP de EE.UU. b. UK Government G-Cloud, una propuesta de Acuerdos Marcos para la computación en la nube en la Administración pública de Reino Unido. c. Canada Right Cloud, la adopción de la nube solo cuando es necesario. d. Grupo de Trabajo IV (Comercio Electrónico) de la Comisión de las Naciones Unidas para el Derecho Mercantil*

CAPÍTULO III – INICIATIVAS LEGALES

a. Anteproyecto de Ley de Código Mercantil Español

a. *Introducción. Principios comunes y específicos en el marco del comercio electrónico*

En el aprobado Anteproyecto de Ley de Código Mercantil[133], de 30 de mayo de 2014, era obligatorio hacer mención expresa a los procesos de contratación electrónicos, cada vez más instaurados en una sociedad globalizada y claramente "electronificada". Por ello, el Capítulo I del Título II (de las formas especiales de contratación) del Libro IV se dedica de manera exclusiva a la contratación electrónica. Si bien, haciéndonos eco de las palabras de MADRID[134], no se consagra en el Código la denominación "contrato informático" y "contrato electrónico" aunque tipifique y regule dos clases de contratos informáticos, así como establece una regulación general para la contratación electrónica. PERALES VISCASILLAS[135] recalca que la ubicación en el Anteproyecto no resulta baladí, dota a su contenido de aplicación transversal a la amplia gama contractual recogida en el Código, siempre que utilicen medios electrónicos para la formación, perfección, administración, cumplimiento y extinción de los contratos, artículo 421-1.1, pudiendo modificar o concretar las normas de la teoría general de los contratos. De esta forma, lo relevante para la aplicabilidad de la regulación que contiene es el empleo de medios electrónicos para la contratación, pudiendo ser aplicable, por tanto, el contenido a la distinta tipología contractual recogida en este Título ("formas especiales de contratación").

De forma directa, a través de los contratos tipificados, o de forma indirecta, mediante la calificación de los contratos informáticos, el Anteproyecto pretenden cubrir la pluralidad de contratos informáticos que aparecen en el tráfico comercial. SÁNCHEZ

---

[133] http://servicios.mpr.es/seacyp/search_def_asp.aspx?crypt=xh%8A%8Aw%98%85d%A2%B0%8DNs%90%8C%8An%87%99%7Fmjro%86og%A3%91. Último acceso: 08.08.2018.

[134] MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 72.

[135] PERALES VISCASILLAS, Pilar: "La contratación electrónica en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295 (Enero-Marzo 2015), p. 3 (edición electrónica del capítulo por Proview™).

DEL CASTILLO[136] dictamina que *"de aprobarse el Código con su redacción actual, el ordenamiento jurídico español zanjará en gran parte algunas de las inseguridades que hasta el día de hoy permean a los operadores legales y destinatarios del entramado que da base a la LSSICE[137]"*.

En el Capítulo II apartado a) de nuestro estudio ya hacíamos referencia a las distintas opiniones vertidas sobre la contratación automática y su consideración como medio electrónico, lo que imposibilitaría, según la posición contraria a su condición como medio electrónico, la aplicación de las normas que se recogen sobre la contratación electrónica en el Anteproyecto de Ley de Código Mercantil. Damos por reproducido lo expuesto en el Capítulo de referencia.

Analizando el contenido del Anteproyecto, destaca la plasmación normativa y expresa en el Derecho autóctono de los principios enumerados, y reconocidos en la práctica, para el Derecho electrónico en la Ley Modelo de Comercio Electrónico. Es perentorio el dictado de la Exposición de Motivos V-7, al establecer que "*el Capítulo I de este Título regula la contratación electrónica. Las normas que en él se contienen no son absolutamente nuevas, sino que en parte son el resultado de la recopilación, mejora y puesta al día de disposiciones que se encontraban dispersas en el ordenamiento español. En este Capítulo se ponen en práctica, aunque no los consagre expresamente, los grandes principios de la contratación electrónica, esto es, la equivalencia funcional, la neutralidad tecnológica, la inalteración del derecho preexistente, la libertad de pacto y la buena fe. Al mismo tiempo, es absolutamente respetuoso con el escaso contenido de las Directivas europeas en la materia; de igual modo, se ha inspirado en las muy difundidas Leyes Modelo de CNUDMI/UNCITRAL sobre contratación y firmas electrónicas de 1.996 y 2001 respectivamente*". Aunque en la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico ya se hiciera referencia a los citados principios, en cuanto a la eficacia y el régimen de responsabilidad, sería el primer texto normativo en España que recoja de forma clara los principios rectores del comercio

[136] SÁNCHEZ DEL CASTILLO, Vilma: "Algunas referencias sobre los aportes del Doctor Rafael Illescas Ortiz al Derecho del Comercio electrónico. A propósito de la regulación estatuida en el capítulo de contratación electrónica de la propuesta de Código Mercantil", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, 2015, Universidad Carlos III de Madrid, p. 1845.

[137] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

electrónico. Se hace necesario, por tanto, diseccionar el contenido del Anteproyecto y aflorar la configuración y disposición de este marco regulador[138].

Sirviéndonos de la reflexión que hiciéramos en apartados anteriores[139], el principio de buena fe contractual, básico en el Derecho de obligaciones, no se encuentra reconocido de manera expresa dentro del capítulo que trata el fenómeno de las contrataciones electrónicas o por medios informáticos. Si bien, su manifestación en el artículo 412-2.2 no es óbice para obviar su aplicación dentro de, parafraseando al Anteproyecto, *"las formas especiales de contratación"*. Sí puede resultar extraño la regulación en negativo del deber de las partes en materia contractual[140].

El principio de libertad de forma aparece de forma autónoma en el artículo 413-8, indicando que "*la celebración del contrato por escrito solo será requisito necesario para su validez si la Ley lo establece así expresamente*", principio que debemos vincularlo con el de libertad contractual o, como denomináramos anteriormente, de la autonomía de la voluntad, expresado en el artículo 421-1.3 del tenor de "*la utilización de medios electrónicos en los contratos mercantiles no requiere el previo acuerdo de las partes*". Aparece, nuevamente, en el artículo 421-13. Tal es la importancia del citado principio que la propia Exposición de Motivos recoge que el soporte en el que se materialice el negocio no necesita acuerdo previo entre las partes del contrato[141].

El principio de inalterabilidad del derecho preexistente[142], es decir, la no necesidad de alterar el marco jurídico que regla las relaciones entre sujetos cuando se introduce un nuevo canal de comunicación o, de modo más general, de contratación, se encuentra reconocido en el artículo 421-1.3. Si lo unimos con el principio de neutralidad

[138] El orden de aparición en el presente estudio no responde al expuesto en el Anteproyecto. Se ha seguido, para facilitar la comparación, el establecido en el Capítulo II.d.

[139] Principalmente Capítulo II.d: "Principios comunes y específicos en el marco del comercio electrónico".

[140] De esta forma dispone: *"La parte que hubiera negociado o interrumpido las negociaciones con mala fe será responsable por los daños causados a la otra parte. En todo caso se considera mala fe el hecho de entrar en negociaciones o de continuarlas sin intención de llegar a un acuerdo".*

[141] Exposición de Motivos V-8.

[142] Remitimos al Capítulo II. d, donde se argumenta la conveniencia de la inalterabilidad o inalteración del derecho preexistente y la relatividad actual del principio cuando se relaciona con las nuevas tecnologías.

tecnológica, regulado en el artículo 421-4.3[143], se puede apreciar cómo en la redacción del Anteproyecto se es consciente de la evolución continua del fenómeno tecnológico y cómo debe apropiarse, es decir cómo se debe nutrir, este nuevo medio de contratación sin necesidad de crear un modelo jurídico propio. Este último principio se presenta como novedoso al reconocerse expresamente en un texto normativo de aplicación. Tanto es así que incluso en la Ley Modelo de Comercio Electrónico aparecía redactado de forma difusa.

El principio de no discriminación aparece definido en el artículo 421-1.1[144]. Lo más característico de la formulación en el Anteproyecto, en comparación con la Ley Modelo de Comercio Electrónico, alma mater del texto normativo, es la consideración de *"salvo disposición expresa legal en contrario"*. Por lo tanto, no hay un pleno reconocimiento de las comunicaciones electrónicas, si bien, dependerá de la propia voluntad del legislador para determinar el alcance de la excepción. La vertiente positiva del principio, equivalencia funcional, aparece a reglón seguido en el artículo 421-1.2[145]. La redacción sigue, desde nuestro punto de vista, la buena fórmula ya establecida en la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, dado que, de forma global, no como propone la Ley Modelo de Comercio Electrónico, dicta que "*siempre que la ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico".* Son manifestaciones del principio

[143] *"A los efectos del presente Código, por sistema de información se entenderá todo sistema que sirva para generar, enviar, recibir, archivar o procesar de alguna otra forma comunicaciones electrónicas".*

[144] *"Toda declaración o acto referido a la formación, perfección, administración, cumplimiento y extinción de los contratos mercantiles podrá efectuarse mediante comunicación electrónica entre las partes y entre estas y los terceros, salvo disposición expresa legal en contrario".*

[145] *"Siempre que la ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico".*

de equivalencia funcional lo expuesto en el artículo 421-7[146], titulado documento y firma electrónicos, y el artículo 421-9[147], que desarrolla la factura electrónica.

b. Tipificación de los contratos de comunicaciones electrónicas

Teniendo como sustrato el régimen jurídico determinado por los principios rectores, el Anteproyecto se ocupa de dos figuras concretas y de disposiciones generales para los contratos de comunicaciones electrónicas, a saber, el contrato de servicio de comunicaciones electrónicas, el contrato de alojamiento de datos y los acuerdos para la copia temporal de datos o de información, si bien este último con escasa profundidad.

Lo primero que debe reseñarse, con carácter general, es la declaración de mercantilidad que hace el Anteproyecto de los contratos aquí tratados. Teniendo en cuenta el artículo 001-3.1.b) el cual recoge que serán mercantiles, quedando sujeto a las normas del presente Código (actualmente Anteproyecto), *"los actos y contratos que, por razón de su objeto o del mercado en que se celebren, el Código califica de mercantiles"*, el artículo 532-1.1 nos recalca que todos los contratos para las comunicaciones electrónicas serán siempre mercantiles. De esta forma, despeja las dudas que pudiera suscitar los contratos en razón de los sujetos intervinientes y las distintas formas jurídicas a adoptar.

En otro orden de cosas, y siendo conscientes de la evolución constante que sufre la electronificación y con el objetivo de no encorsetar las distintas formas de negocio a los contratos tipificados en el Anteproyecto, establece que *"salvo en lo que resulte incompatible con su contenido o finalidad, serán de aplicación al contrato de alojamiento de datos y obligación de realizar copias de carácter temporal las disposiciones relativas al contrato de servicio de comunicación electrónica"*, por lo tanto, como veremos, se configura como modelo regulador de los contratos de prestación de los servicios informáticos. La primera salvedad aparece en el propio artículo 532-1.3 del Anteproyecto.

---

[146] "*1. Toda comunicación electrónica goza de la naturaleza de documento electrónico de acuerdo con las disposiciones aplicables de la legislación sobre firma electrónica.*
2. Toda comunicación electrónica emitida con fines negociales habrá de poder ser atribuida a su emisor. A tal fin, salvo disposición o pacto en contrario, podrá ser utilizada una firma electrónica apropiada a los fines perseguidos y las circunstancias del caso".

[147] *"La factura emitida mediante comunicación electrónica equivale funcionalmente a la factura emitida en soporte papel, produciendo idénticos efectos siempre que reúna los requisitos que le son legalmente exigibles, mantenga la integridad de su contenido y pueda ser atribuida indubitadamente a su emisor".*

i. Contrato de servicios de comunicación electrónica

El contrato de servicio de comunicación electrónica aparece definido en el artículo 532-2, le precede el modelo de los contratos de prestación de servicios informáticos, estableciendo que *"por el contrato mercantil de servicio de comunicación electrónica el prestador, a cambio de una remuneración, se obliga frente al cliente a suministrarle el acceso a la red pública de comunicaciones electrónicas para la transmisión de datos o información"*. Resulta innecesaria, como dice GALÁN CORONA[148], la reiteración de la naturaleza mercantil del contrato, pues no caben contratos de servicios de comunicación electrónica con otra naturaleza respetando las disposiciones generales aplicables a estos contratos.

El objeto del contrato queda determinado por el acceso a la red con el fin de transmitir datos o información[149]. Aunque en su redacción no se recoja de manera expresa, claramente se refiere, como así considera MADRID[150], al acceso al conglomerado de redes que configura Internet. Sin embargo, para poder delimitar el concepto objeto de estudio debemos acudir a la Ley 9/2014, de 9 mayo, de Telecomunicaciones[151]. El artículo 2.1 de la Ley de Telecomunicaciones recoge el interés general de las redes, con independencia de la titularidad de las mismas. Establece expresamente los *"derechos de los operadores y despliegue de redes públicas de comunicaciones electrónica"* entre los artículos 29 y 38, y lo más definitorio, *"derechos específicos de los usuarios finales de redes y servicios de comunicaciones electrónicas disponibles al público"*, artículo 47, que debe completarse con el contenido mínimo determinado en el contrato, artículo 53.

---

[148] GALÁN CORONA, Eduardo: "Contrato de servicios mercantiles y contrato de servicios electrónicos en el Anteproyecto de Código Mercantil", *Hacia un Nuevo Código Mercantil*, 2014, Thomson Reuters Aranzadi, p. 426.

[149] ASENSI MERÁS define la conexión a Internet, desde un punto de vista técnico, como *"una realidad física que permite la conexión de la red privada del usuario a través de un conjunto de estándares y procesos a la red del operador y, a través de esta, al conjunto de redes que integran Internet"* (ASENSI MERÁS, Altea: "Los contratos para las comunicaciones electrónicas", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, 2015, Universidad Carlos III de Madrid, p. 1198).

[150] MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 83.

[151] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950. Último acceso: 08.08.2018.

El contrato requiere, como contraprestación del cliente, una remuneración. Esta debe ser, según el artículo 531-1 del Anteproyecto, en dinero, tendente a satisfacer las necesidades del prestador del servicio.

Más complejo de analizar pueden ser las restantes obligaciones de las partes. Las obligaciones para el prestador del servicio se recogen en el artículo 532-3[152]. La actividad debe posibilitar al cliente, que puede ser cualquier persona física o jurídica y pública o privada, acceder a una red pública de comunicaciones electrónicas para la transmisión de datos o información. MADRID[153] reseña aquí una cuestión primordial, qué debe entenderse por datos o información. Con el avance tecnológico y las posibilidades de comunicación no sería oportuno excluir del concepto de información, e incluso de datos, la transmisión de voz, sea cual sea el medio a través del cual se transmite. Otra cuestión sería incluir prestaciones adicionales, como puede ser el alojamiento de datos, cláusulas también reguladas en el Anteproyecto.

Es obligatorio que se convenga en el contrato las condiciones de *continuidad, regularidad, velocidad, volumen y seguridad* a las que debe atender el prestador del servicio, o en su defecto, atender a los estándares normales de desarrollo o lo contemplado en los códigos de conducta o instrumentos análogos publicados. Debe tenerse siempre presente que, aunque no se hubiera dicho nada en el contrato, las condiciones antes reseñadas sobre el acceso a la red y la transmisión de información debe responder a los estándares normales en el desarrollo de actividades análogas en el mercado, al imperar en materia contractual el principio de buena fe. Por lo tanto, estamos ante un contrato de tracto sucesivo, que obliga necesariamente a una obligación de resultado, *"acceso a la red pública"*, al ser esencial para la prestación del servicio[154]. El estudio de las

[152] Artículo 532-3: *"1. El prestador estará obligado a proporcionar el acceso a la red pública de comunicaciones electrónicas para la transmisión de datos o información, en las condiciones de continuidad, regularidad, velocidad, volumen y seguridad previstas en el contrato y, en lo no previsto, en las condiciones y bajo los usos y los estándares normalmente observados en la prestación de servicios idénticos o análogos, así como en los contemplados en los códigos de conducta o instrumentos análogos publicados o adheridos por el prestador.*
2. El prestador o estará obligado a mantener el secreto de las comunicaciones."

[153] MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 84.

[154] En contraposición de lo que dictamina el Anteproyecto para los contratos de prestación de servicios mercantiles en el artículo 531-1.

obligaciones que recaen en el prestador deben completarse con las que aparecen establecidas en la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico [155].

Por último, el Anteproyecto recoge que debe mantenerse el secreto en las comunicaciones, en concordancia con el régimen establecido la Ley de Telecomunicaciones[156]. MADRID[157] nos muestra cómo esta obligación vincula a todos los operadores o prestadores del servicio que intervienen en la transmisión electrónica, independientemente de que sean operadores de redes o no, a tenor de la obligación *ex lege*. Como matiza ASENSI MERÁS[158], el cumplimiento de la obligación relativa al secreto de comunicaciones resulta aplicable también en el ámbito extracontractual, porque la cláusula de exoneración contenida en el artículo 14 de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico exige que no sean *"responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos"*.

Termina haciendo una previsión el Anteproyecto, en modo de obligación del prestador de servicios, para poner a disposición del cliente los medios o equipos técnicos que permitan hacer posible la comunicación electrónica. Qué duda cabe que la obligación que recae sobre el prestador de servicios tiene como razón de ser el propio conocimiento de la entidad especializada en los requisitos técnicos que permiten realizar las comunicaciones con las características y especificidades que le son propias, dependiendo de equipos para la conexión a la red suministrados al propio servicio contratado. De esta forma, el Anteproyecto intenta garantizar, con independencia de que el contrato pudiera contener una cláusula específica, que debe ser el prestador de servicios quien atienda a estos requerimientos, como obligación que recae en esta parte del contrato. Esta

[155] Véase, entre otros, el artículo 10 y 12.bis de la Ley.

[156] En concreto, el artículo 39.1 establece: *"los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias"*.

[157] MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 91.

[158] ASENSI MERÁS, Altea: "Los contratos para las comunicaciones electrónicas", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, 2015, Universidad Carlos III de Madrid, p. 1200-1201.

regulación no abarca al régimen que tutelará esa puesta a disposición, pues como bien dice el artículo 532-4 del Anteproyecto, la puesta a disposición se reglamentará por el título que rija la puesta a disposición de los equipos, que requerirá o no la transmisión de la propiedad.

La contraposición a las obligaciones del prestador del servicio son las que se recogen en el artículo 532-5, referente a las obligaciones que recaen en el cliente. Estas pueden resumirse en pagar la remuneración por el acceso proporcionado según lo pactado o, en su defecto, según los usos del sector; utilizar el servicio conforme a la regulación contenida en el contrato, siempre respetando el derecho de terceros, a la ley y al orden público; y salvaguardar el secreto de cualquier instrumento o medida de seguridad. Por las características del servicio suministrado, la obligación principal del cliente se realizará en pagos sucesivos, como pueden ser en períodos de mes a mes. El artículo 532-5 vuelve a reproducir el criterio convencional del artículo 531-5 del Anteproyecto. Importantes son las dos premisas restantes, en primer lugar, porque el cliente tiene limitada su actuación en la red, exigiendo una conducta que no infrinja los derechos que pudieran estar conexos. A lo que habría que añadir, vinculado a la tercera de las obligaciones indicadas, el actuar conforme a la buena fe contractual, debiendo comunicar el cliente los cortes, interrupciones o las deficiencias del servicio y las incidencias que pudieran suceder en las claves o sistemas de autentificación o seguridad en el acceso. De otra, cliente y prestador podrían estar desprotegidos por actuaciones de terceros que podrían vulnerar las medidas impuestas por el prestador o podría crear una falsa apariencia de actuación del cliente.[159][160]

[159] Habría que incidir en las obligaciones que el Anteproyecto impone a los clientes en la prestación de los servicios mercantiles en general, entre las que se incluyen la de proporcionar la información que resulte precisa para el correcto cumplimiento de la obligación por parte del prestador del servicio y de colaborar en la medida en que se le requiera, artículo 531-3 del Anteproyecto.

[160] Discutible es la posición que sigue ASENSI MERÁS, al considerar que no muta la naturaleza jurídica del contrato el supuesto de que el usuario pueda conectarse a Internet de forma gratuita (ASENSI MERÁS, Altea: "Los contratos para las comunicaciones electrónicas", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, 2015, Universidad Carlos III de Madrid, p. 1201). Lo que caracteriza a los contratos de comunicaciones electrónicas, en las obligaciones referentes al cliente, es precisamente el pago por el servicio, siendo una obligación necesaria para tal consideración. Por lo tanto, ante un servicio gratuito, conforme al artículo 531-1 del Anteproyecto, las partes no estarán amparadas en el marco contractual recogido por el Anteproyecto, debiéndose atender a las responsabilidades que la propia LSSICE establece para los prestadores de servicios, al incidir en que las actividades del prestador representen una actividad económica, pudiendo tener el servicio carácter gratuito.

El sistema de responsabilidad contractual para los contratos de servicio de comunicación electrónica se regula en los artículos 532-6, 532-7 y 532-8, ante el incumplimiento del prestador de servicios, y el artículo 532-9, para el incumplimiento del cliente. Tanto para el supuesto del incumplimiento de las obligaciones derivadas del contrato por el prestador del servicio como por el cliente, el Anteproyecto exige a las partes una actuación culposa para que pueda ser imputable y se derive la correspondiente indemnización a la contraparte.

Tratando la responsabilidad del prestador, es destacable como se invierte la carga de la prueba y como el cliente asume el riesgo de un servicio defectuoso siempre que no sea debido a la culpa del proveedor o sus auxiliares. Por lo tanto, los previsibles daños que pudieran producirse por el incumplimiento del prestador de servicios, o sus auxiliares, es asumido por cliente. Además, al limitarse la responsabilidad a la culpa del prestador o sus auxiliares, la deficiente actuación de terceros ajenos a la vinculación del contrato también recae en el consumidor. La norma, sin género de dudas, es protectora a los proveedores de acceso. Interesante sería que en el Acuerdo de Nivel de Servicio pudiera delimitarse de manera proporcional a las partes el incumplimiento de la obligación principal[161].

La regla general de responsabilidad se matiza en los artículos 532-7 y 532-8, al tratar los supuestos específicos de incumplimiento y la interrupción del servicio. Recoge tres casos:

- No será responsable el prestador de servicios de la interceptación de la información transmitida o de cualquier intromisión ilegítima de terceros siempre que pruebe que ha aplicado todas las medidas de seguridad técnicamente apropiadas para tal fin. Se presume, por tanto, que el prestador no tiene la culpa del ataque ilegítimo de terceros en la obligación de secreto. Queda por delimitar qué debe entenderse por las medidas apropiadas y la extensión de las mismas.

[161] Para completar el correcto estudio de la responsabilidad del prestador de servicios, sería oportuno atender a la regulación contenida en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, especialmente la relacionada con los operadores de redes y proveedores de acceso (artículo 14), si bien, solo discrimina en referencia a la "información transmitida", no a la obligación principal de acceso. Para un estudio más completo: PLAZA PENADÉS, Javier: "La responsabilidad civil de los intermediarios en internet y otras redes", *Contratación y comercio electrónico*, 2003, p. 195-237; y RODRÍGUEZ DE LAS HERAS BALLELL, Teresa: "Intermediación en la red y responsabilidad civil", *Revista Española de Seguros*, 2010, núm. 142, p. 217-259.

- Será responsable el prestador de servicio de la pérdida de la integridad de la información transmitida siempre que el cliente pruebe la actuación culposa del prestador. Lo relevante resulta en la presunción de culpa del prestador, dado que, si las partes han acordado o el prestador ha comunicado al cliente las medidas de seguridad para salvaguardar la integridad de la información, será este responsable siempre que algunas de las medidas no hayan sido aplicadas[162][163].
- A pesar del claro incumplimiento del contrato por parte del prestador del servicio, no incurrirá en responsabilidad por la interrupción del servicio cuando sea necesaria por razones de mantenimiento de la regularidad del servicio o del equipo necesario para la prestación, siempre que trasmita al cliente en tiempo y forma las interrupciones, teniendo una actitud diligente si no se reseñó tal extremo en el contrato; y, en otro lugar, no será responsable si la interrupción reside en la red de comunicaciones electrónicas siempre que el prestador no sea operador de la red y siempre que no hubieran podido ser evitadas por el prestador con una actitud diligente. Son, por tanto, excepciones a la obligación general del prestador de servicio.

Los artículos 532-8.3 y 532-8.4 vienen a determinar cómo considerar los incidentes que pueden ocurrir en las interrupciones del servicio. De forma general, cuando se produzcan interrupciones múltiples serán consideradas como una única interrupción si impiden al cliente la comunicación o transmisión de la información en condiciones normales, por su periodicidad o reiteración. Por otra parte, si las partes lo han pactado, el prestador no responderá de los daños que produzcan las interrupciones del servicio con anterioridad a la comunicación del cliente, matizando que estas deberán ser injustificadas. En caso contrario, será responsable desde el momento en el que tenga lugar la interrupción del servicio. El Anteproyecto vuelve a ofrecer mayores garantías al prestador del servicio que al cliente, acotando su responsabilidad ya sea de manera general o pactada,

[162] En este sentido, no podemos olvidar que el artículo 12bis.2 de la Ley 34/2002 de servicios de la sociedad de la información y del comercio electrónico establece la obligación de información de seguridad a los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares, debiendo *"informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios"*.

[163] MADRID, en el estudio sobre la determinación de ser la presunción absoluta o relativa, considera que al establecerse un régimen específico constituye una excepción al régimen general de la responsabilidad establecido en el artículo 532-6, por lo que será responsable el prestador de servicios siempre que no aplique todas las medidas de seguridad previstas (MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 99-100).

recordando el escaso poder negociador de los usuarios del servicio. No estamos ante una obligación de medios en el contrato de servicios de comunicación electrónica, aunque el legislador pretenda excluir gran parte de los condicionantes que intervienen para considerar de resultado la prestación, tanto es así, que deberá atenderse a las cláusulas particulares y a los Acuerdos de Nivel de Servicios que se establezcan para determinar la responsabilidad por la interrupción o ruptura del servicio.

Tras las obligaciones del cliente recogidas en 532-5 del Anteproyecto, el artículo 532-9 regula la responsabilidad contractual del cliente. Con una cláusula general, correlativa a la dispuesta para el prestador de servicios en el artículo 532-6, el Anteproyecto dicta *"el cliente deberá indemnizar al prestador los daños causados por el incumplimiento de sus obligaciones derivadas del contrato. Quedará el cliente exonerado de su responsabilidad si prueba que el incumplimiento no es imputable a su culpa ni a la de sus auxiliares"*. Más concreta es la recogida en su punto segundo, relativa a los medios o medidas de seguridad y las condiciones de uso. De esta forma, el cliente responderá, debiendo indemnizar al prestador por daños del uso del servicio por terceros, cuando se hubieren aplicado las medidas de seguridad para la identificación o de restricción de acceso y se incumplan las condiciones de uso por parte del cliente. Lo relevante en la regulación propuesta es el especial deber que recae sobre el cliente, porque incluso en el acceso por el tercero no consentido se hace responsable al cliente. No es, por tanto, un incumplimiento material de las obligaciones que recaen en el cliente, ni una actuación culposa o negligente del cliente, solo traslada al cliente el riesgo de las actuaciones ilícitas del tercero, a una de las partes del contrato, una vez más, la más débil.

Sin querer extendernos en demasía, el contrato se entiende celebrado por tiempo indefinido, salvo pacto o acuerdo en contrario, pudiendo las partes denunciarlo unilateralmente con un preaviso escrito de treinta días, artículo 532-10, no exigiendo causa para la resolución[164]. Por consiguiente, este preaviso solo será exigible, salvo acuerdo en contrario, cuando no se haya pactado duración definida o se haya omitido tal extremo en el contrato[165]. Termina la sección 2ª del Capítulo II con el supuesto de

[164] Preaviso que no se recoge en la regulación general recogida en el artículo 531-7 del Anteproyecto.

[165] Qué duda cabe que en la práctica contractual los prestadores de servicios pueden establecer distintas cláusulas referentes a la duración del contrato. Por ejemplo, es común que establezcan cláusulas de permanencia como contraposición a la asunción de costes de los servicios cedidos al cliente o establezcan

resolución automática del contrato, cuando el prestador del servicio quede privado de la posibilidad de continuar con el servicio por la pérdida del título o la habilitación administrativa necesaria. Sin embargo, para corresponder indemnización económica por daños y perjuicios al cliente, la imposibilidad indicada debe haberse producido mediando culpa o dolo por parte del prestador del servicio. En caso contrario, el cliente vuelve a asumir la carga de verse privado del servicio y las consecuencias perjudiciales que pudieran sobrevenir[166].

ii. Contrato de alojamiento de datos

El segundo contrato tipo aparece definido en los artículos 532-12 y 532-13 del Anteproyecto. El *hosting* posiblemente sea de las prestaciones de servicios más conocidas y utilizadas tras la expansión de Internet al ámbito empresarial y a los usuarios con un nivel medio de conocimientos tecnológicos. Por otra parte, los desarrollos posteriores de los distintos servicios ofertados por las empresas de nuevas tecnologías parten, tienen como base o se sirven del objeto del presente contrato para perfeccionar el servicio e incorporar valor añadido.

La definición de qué debe considerarse como contrato de alojamiento de datos a los efectos del Anteproyecto la encontramos en el primero de los artículos. En términos generales podemos indicar que con el alojamiento de datos se pretende almacenar la información y los datos a través de la conexión con la red de comunicaciones, pudiendo acceder a la información y los datos conservados el cliente y terceros por redes abiertas o cerradas de telecomunicaciones.[167] Como manifiesta MADRID[168], sigue una estructura

---

una duración determinada en el contrato y entienda automáticamente prorrogado por períodos iguales una vez finalizado el plazo inicial si no se comunica la decisión de no prorrogarlo.

[166] Remitimos a un estudio profundo de las causas específicas de extinción de los contratos de prestación de servicios mercantiles en general, establecidas en el artículo 531-8 del Anteproyecto.

[167] Una de las definiciones más extendidas en el ámbito jurídico puede ser la recogida por MARZO PORTERA, Ana y MARZO PORTERA, Iziar*: "*Definición de los contratos informáticos y electrónicos", *Los Contratos Informáticos y Electrónicos. Guía práctica y formularios*, 2004, Ediciones Experiencia S.L., p. 39. Incluye dos características que, a nuestro juicio, no son propias del contrato de alojamiento de datos: en primer lugar, el acceso a las redes de telecomunicaciones, tipificado en otro artículo en el propio Anteproyecto; y la posibilidad del almacenamiento de *software*, lo que posibilitaría no solo el almacenamiento y conservación de datos e información, sino la interactuación y capacidad operativa de trabajo en el alojamiento. Respecto a esto último, supone un valor añadido al contenido esencial del contrato, asimilándose a nuevos servicios tecnológicos. Sobre la definición del contrato, véase SÁNCHEZ LEIRA, Reyes: "Contrato de hospedaje en página web: estructura contractual básica y protección de datos", *Revista de Contratación Electrónica*, 2005, núm. 61, p. 3-30.

[168] MADRID, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295, p. 107.

similar a la noción establecida en el artículo 532-2, regulación general. Por tanto, es un contrato oneroso, de carácter mercantil, sinalagmático y de tracto sucesivo.

Las principales obligaciones que se establecen para el prestador del servicio son, detalladas en el artículo 532-13, las siguientes:

- El prestador de servicios debe poner a disposición del cliente la capacidad de almacenamiento contratada, que se encuentra bajo su control.
- Tiene que conservar los datos y la información almacenada, manteniendo su integridad.
- Debe permitir el acceso a la información y los datos almacenados al cliente y a los terceros, en su caso, a través de la red de comunicaciones electrónicas, previa disposición de los mecanismos de direccionamiento electrónico.
- El sistema debe permitir el acceso a la información, la recuperación, el manejo o la cancelación de los datos y la información almacenada.
- Toda esta serie de obligaciones se regirán según lo pactado en el contrato, y en su defecto, en las condiciones y bajo los usos y los estándares del sector para servicios similares, así como los códigos de conducta o instrumentos similares o adheridos por el prestador.

La principal diferencia, por tanto, que se muestra respecto al objeto del contrato de servicio de comunicación electrónica reside, precisamente, en que ahora el prestador de servicios debe garantizar no solo el acceso a los datos sino la conservación y mantenimiento integro de la información. Su incumplimiento conlleva a la no ejecución del contrato y frusta la finalidad que este persigue. Precisamente por ello, no le es de aplicación la responsabilidad por incumplimiento contractual del prestador del servicio[169]. GALÁN CORONA[170] expone que la principal razón en la diferencia del régimen de responsabilidad del prestador de servicio reside en la distinta naturaleza jurídica del contrato de *hosting* respecto del contrato del servicio de comunicación electrónica, considerando que en este el prestador tiene una obligación de medio y en el

[169] Como se ha señala *ad supra*, en el artículo 532-1.3 del Anteproyecto establece *"no será de aplicación al contrato de alojamiento de datos lo dispuesto sobre responsabilidad del prestador del servicio por incumplimiento"*.

[170] GALÁN CORONA, Eduardo: "Contrato de servicios mercantiles y contrato de servicios electrónicos en el Anteproyecto de Código Mercantil", *Hacia un Nuevo Código Mercantil*, 2014, Thomson Reuters Aranzadi, p. 431.

contrato de alojamiento de datos de resultado. Hemos defendido que la finalidad de ambos tipos contractuales es distinta, sin embargo, eximir de responsabilidad al prestador del servicio por una serie de incidencias en el acceso, siempre que recaigan en terceros, no tiene por qué incidir en la consideración de una obligación solo de medio. La política legislativa claramente ha salvaguardado la posición del prestador del servicio antes que la del cliente, bien por la mecánica de la tecnología bien por el poder de los operadores de telecomunicaciones en la economía, pero el prestador debe garantizar el "acceso a una red pública", aunque como hemos reseñado no de manera absoluta. Tanto es así que en la propia redacción cuando establece los supuestos de responsabilidad por interrupciones en el acceso o las comunicaciones, artículo 532-8, no será de aplicación la eximente cuando el prestador sea operador de red. En consecuencia, no estamos ante una obligación de medios en el contrato de servicio de comunicación electrónica, tiene condicionantes de resultado, que además se completarán con los propios que acuerden en las cláusulas particulares y en los Acuerdos de Nivel de Servicios que se establecen comúnmente en el sector.[171]

Serán de aplicación las obligaciones del cliente y su correspondiente responsabilidad por incumplimiento contenidas en la regulación para el contrato de servicio de comunicación electrónica.

iii. Acuerdos para la copia temporal de datos o información.

Por último, el Anteproyecto contempla la posibilidad, potestativo, de contratar la realización de copias temporales de datos o de información. De esta forma, el artículo 534-14 recoge la siguiente obligación del prestador del servicio:

a) A realizar copia de la información o los datos conforme a las indicaciones del cliente, o bien de manera automática cuando ello resulte necesario, para su conservación con carácter temporal y su transmisión a través de la red de comunicaciones electrónicas, con vistas al acceso de los terceros que lo soliciten a tales datos o información.

b) A actualizar periódicamente la copia de los datos o la información, al objeto de respetar su contenido en cada momento, en las condiciones previstas en el

[171] Para completar el régimen de responsabilidad del prestador del servicio en los contratos de alojamientos de datos debe de acudirse al artículo 16 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

contrato o, en lo no previsto, en las condiciones y bajo los usos y los estándares normalmente observados en la prestación de servicios idénticos o similares, así como en los contemplados en los códigos de conducta o instrumento análogos publicados o adheridos por el prestador.

Lo primero que debe destacarse es que los redactores no han contemplado la posibilidad de que la obligación de realizar las copias temporales se configure como un contrato autónomo, al limitar el régimen establecido *"cuando en el contrato de servicio de comunicación electrónica o en el contrato de alojamiento de datos se obligue"*.

La regulación resulta parca, delimitándose por lo dispuesto en los contratos de servicios de los que depende, siendo además de aplicación el régimen de responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios en el artículo 15 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.[172]

Dentro de las cláusulas de los acuerdos para la copia de datos o información pueden quedar incluidos los necesarios en la indexación de contenidos de páginas webs que se utilizan en los motores de los proveedores para los servicios de búsqueda por Internet, incorporando datos en la memoria caché.

c. Incidencia del Anteproyecto de Ley de Código Mercantil en la contratación del cloud computing

Por las características esenciales del contrato de computación de la nube es recurrente acudir a la figura jurídica del contrato de *hosting* para paliar el vacío legal que presenta actualmente el servicio tecnológico. Tanto es así, que en la definición que algunos autores hacen del contrato de alojamiento de datos introducen elementos esenciales que no le son propios, o al menos, no son elementos esencialmente definitorios[173]. Posiblemente, la asimilación de los conceptos trae causa de la amplia y primitiva expansión del modelo de

[172] En la Exposición de Motivos (II) de la citada Ley se recoge como actividades de intermediación *"la realización de copia temporal de las páginas de Internet solicitadas por los usuarios"*, así como en el Anexo en Definiciones, b) "servicios de intermediación", son *"servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet"*.

[173] Anteriormente hemos matizado la definición de *hosting* de MARZO PORTERA, Ana y MARZO PORTERA, Iziar.

implantación de la nube como infraestructura de servicio (*IaaS*). La expansión del *cloud computing* como un servicio por el cual las empresas y los usuarios mantienen datos e información en el *hardware* del prestador del servicio permitía un ahorro considerable en costes, pero limitaba y limita la interactuación de los usuarios finales. Se hacía necesario, por tanto, plataformas o *software* que facilite la comunicación con el servicio de la nube. Además, muchos de los servicios prestados no se correspondían con un modelo *IaaS,* al empaquetar los datos y la información o presentar una aplicación para agilizar la transmisión.

Otro aspecto importante es que, a través del contrato de computación en la nube, y así coinciden las diferentes acepciones del servicio, como señalábamos en el Capítulo I, el proveedor de servicios debe garantizar el acceso de los usuarios a través de Internet a la capacidad informática contratada. A lo que habría que añadir, que no solo se limita al almacenamiento de datos, sino que coinciden en que hay una especie de tratamiento o utilización de los datos. Estas características, por tanto, lo diferencian del contrato de alojamiento de datos.

Se ha señalado como elemento esencial en los contratos de comunicaciones electrónicas definidos en el Anteproyecto la necesidad de remuneración económica por parte del cliente. La experiencia nos demuestra que, sobre todo en los supuestos de contratación por parte de usuarios no vinculados a la práctica empresarial o gubernamental, se ofrecen los servicios no de manera gratuita pero sí con una contraprestación que no es económica.

Independientemente del modelo de implantación de la nube, las previsiones recogidas en el contrato de aplicación general, servicio de comunicación electrónica, encuentra un elevado acomodo con la regulación del servicio del *cloud*. Reseñamos, que, si la implantación de la nube se centra exclusivamente en el alojamiento de datos e información, nada impide la aplicación de lo determinado para el contrato de alojamiento de datos e información en el Anteproyecto.

Las obligaciones que residen en el prestador de servicios, que se determinarán según el modelo de implantación y el modelo de computación en la nube, dependiente de la titularidad, control y gestión del servicio, debe posibilitar al cliente, como mínimo, el acceso a través de Internet al almacenamiento de datos e información, así como al *software* en ordenadores remotos del prestador de servicio, posibilitando una capacidad

informática a voluntad del cliente. De esta forma, el servicio bajo demanda, el acceso al ancho de banda, la elasticidad y rapidez en la provisión del servicio y la mensurabilidad del servicio exigen que para el contrato de computación en la nube sea necesario convenir condiciones de *continuidad, regularidad, velocidad, volumen y seguridad*, condicionantes establecidos para el prestador del servicio en el artículo 532-3 del Anteproyecto. Sin embargo, y a modo de aclaración, el fin del contrato en ambos casos es completamente distinto y la contratación de uno de los servicios regulados al prestador de servicios no implica necesariamente el desarrollo del otro.

Se complementa con el deber de secreto en las comunicaciones, también regulado en el Anteproyecto, acorde con la Ley de Telecomunicaciones. La finalidad con la que se emplea el servicio de la nube es dotar a las empresas, administraciones y usuarios de una capacidad informática escalable según las necesidades y en continuo acceso a través de la red, lo que previsiblemente conlleva el traslado a los recursos del proveedor del servicio, o al *hardware* donde se alojen materialmente, datos e información relevante e incluso de carácter confidencial, sin contar con la protección específica de los datos. Lo que determina, por tanto, que la previsión del secreto de comunicaciones deba imponerse a todos los intervinientes en la prestación del servicio, sea parte contractual o no. Menor relevancia tiene el régimen sobre la disposición de los medios o equipos técnicos que debe proveer el prestador al cliente, pues principalmente la comunicación y acceso en el servicio de *cloud* se realiza a través de un *browser* o navegador web[174].

Respecto a las obligaciones que residen en el cliente, conforme al artículo 532-5 del Anteproyecto, serían perfectamente aplicables con la salvedad indicada de la remuneración económica por la prestación del servicio. Especialmente importante es la correcta actuación del cliente en la ejecución del servicio, pues esta herramienta informática ha sido utilizada en la práctica para infringir derechos relacionados con la propiedad intelectual[175]. Por tanto, el *cloud computing* comparte con la regulación

[174] Actualmente, sin embargo, se observa que los distintos prestadores de servicio en la nube están facilitando a los clientes *software* que facilita la conexión automática a sus servicios contratados, una sincronización en paralelo o el trabajo directo desde el archivo en la nube a través de una conexión directa. Por ejemplo, la aplicación OneDrive para empresas de Microsoft (https://onedrive.live.com/about/es-es/business/), ejecutable en PC y dispositivos móviles, permite el trabajo directo desde documentos alojados en la nube o el trabajo en local y sincronización automática de archivos una vez finalizada la sesión.

[175] El caso más relevante y conocido puede ser el de MegaUpload, servicio para el alojamiento de datos, que evolucionó al sistema de *cloud computing*, cerrado por el FBI en enero de 2012 por infracción de los derechos de autor. Se puede acceder al auto de procesamiento a través del portal de The Wall Street Journal:

establecida en el Anteproyecto las principales obligaciones del cliente: la remuneración por los servicios prestados, el cumplir con la AUP y el deber de colaboración, conforme a la buena fe contractual, informando de los cortes, interrupciones o deficiencias del servicio o de los sistemas de autentificación o seguridad.

Creemos que lo más importante será determinar cómo compatibilizar las responsabilidades del prestador y del cliente. La exigencia de una actuación culposa por parte del prestador o sus auxiliares, como recogen los artículos 532-6, 532-7 y 532-8 del Anteproyecto, propiciarán una mayor expansión del servicio en cuanto a la oferta, pero reducirá, sobre manera, la transición y la confianza de los clientes a esta nueva tecnología. La atipicidad y la naturaleza compleja del servicio de computación en la nube obliga a tener especial diligencia en la aceptación de los Acuerdos de Niveles de Servicio (ANS o SLA) en la contratación. En estos acuerdos, el cliente podrá equilibrar el riesgo a asumir por un servicio defectuoso. Piénsese en la incidencia empresarial que puede tener no poder acceder a los datos e información de grandes compañías por un período de tiempo considerado, más peligroso puede ser incluso el ataque o el acceso por parte de terceros. No podemos olvidar, que esta externalización del servicio hace que algunos prestadores localicen físicamente su *hardware* en países fuera del ámbito comunitario o *safe harbor*. Sin embargo, son grandes entidades las que prestan el servicio de *cloud*, por lo que la capacidad de negociación suele ser limitada, de ahí que debiera reconsiderase la responsabilidad del prestador del servicio. Por este motivo, y dado que algunos modelos de implementación de la nube tienen una naturaleza similar, parece oportuno extender la salvaguarda del artículo 532-1.3, y no ser de aplicación lo dispuesto sobre la responsabilidad por incumplimiento para el prestador de servicios.

Dado el carácter complejo de la computación en la nube, obligaciones que se recogen para el contrato de *hosting* pueden ser perfectamente predicables, aunque este contrato no tenga carácter de aplicación subsidiaria como el contrato de servicio de comunicaciones electrónicas. A saber:

- La disposición de la capacidad contratada, a lo que habría que añadir las posibilidades de escalabilidad.
- El deber de conservar los datos y la información almacenada en su integridad.

https://www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf Último acceso: 08.08.2018.

- El acceso a la información y datos almacenados, por clientes y terceros, a través de los protocolos indicados por el prestador.
- El acceso, recuperación, manejo y la cancelación de los datos e información almacenada.
- La confidencialidad en los datos almacenados, incluso finalizada la prestación del servicio.

Por la relevancia que está adquiriendo el servicio informático y la expansión al ámbito empresarial y profesional, en dispositivos móviles y en ordenadores, e incluso a través del denominado Internet de las Cosas, es necesario que la redacción definitiva del futuro Código mercantil incluya, al menos, una regulación básica sobre los acuerdos en el servicio.

b. Actividad del Grupo Europeo de Protección de Datos "artículo 29"

a. Introducción: qué es el Grupo de Trabajo del artículo 29 y contexto en la prestación del servicio del cloud computing.

El Grupo Europeo de Protección de Datos del artículo 29, también denominado Grupo de Trabajo del artículo 29 (GT 29), nace tras la aprobación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En concreto, el artículo 29 dictamina que *"se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado «Grupo». Dicho Grupo tendrá carácter consultivo e independiente"*, indicando que estará compuesto *"por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión. Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, estas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios"*. En la actualidad, por tanto, son parte los organismos

encargados de la protección de datos de cada uno de los Estados miembros, el Supervisor Europeo de Protección de Datos[176] y la Comisión Europea.

Como resume la Agencia Española de Protección de Datos (AEPD)[177], las funciones principales que encomienda la Directiva 95/46/CE del Parlamento Europeo y del Consejo son estudiar la aplicación de las disposiciones nacionales relacionadas con la aplicación de la Directiva de referencia, la emisión de dictámenes sobre la materia y en concreto sobre los niveles de protección, ser órgano asesor y consultivo de la Comisión Europea para cualquier modificación de la Directiva, y realizar recomendaciones sobre los asuntos relacionados con la protección de datos en el seno de la Unión Europea, debiendo elaborar un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros[178].

El Grupo de Trabajo analiza, por primera vez, la temática del *cloud computing* con el Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012[179]. La investigación tiene un objetivo amplio: analizar todas las cuestiones relacionadas con los proveedores de la computación en la nube en materia de protección de datos, diseccionando la aplicabilidad de los principios recogidos en la Directiva europea sobre protección de datos y sobre privacidad[180]. Son bastante ambiciosas las metas que se

---

[176] El objetivo principal del Supervisor Europeo de Protección de Datos (SEPD) es garantizar que, a la hora de tratar datos personales, las instituciones y organismos de la UE respeten el derecho a la intimidad de los ciudadanos. En la actualidad el Supervisor es Giovanni Buttarelli y el Supervisor adjunto Wojciech Wiewiórowski. Más información en: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_es. Último acceso: 08.08.2018.

[177] Accesible en: https://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php. Último acceso: 23.06.2016.

[178] Las funciones del Grupo de Trabajo se encuentran recogidas de manera extensa en el artículo 30 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo. En este sentido, en el artículo 15.3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas establece que *"el Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE, ejercerá también las funciones especificadas en el artículo 30 de dicha Directiva por lo que se refiere a los asuntos objeto de la presente Directiva, a saber, la protección de los derechos y las libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas"*.

[179] Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf. Último acceso: 08.08.2018.

[180] En concreto, nos referimos, respectivamente, a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y a la Directiva 2002/58/CE del

impone el Grupo de Trabajo, porque como se podrá observar en la práctica, los proveedores tienden a modificar su sistema lógico y normativo con bastante asiduidad, dificultando la tarea de evaluar los riesgos en la materia. Por otra parte, deben ser las instituciones, públicas o privadas, quienes contraten los servicios en la nube, las que evalúen de forma detallada los riesgos que supone contratar la tecnología, por cuanto aspectos como la puesta en común de recursos, la trasparencia, el conocimiento de la cadena de contratistas y subcontratistas encargados del tratamiento, la portabilidad y la localización de los servidores, entre otros, determinarán la conveniencia en la elección del proveedor del servicio. Por lo tanto, este Dictamen puede servir de guía para analizar la amplia oferta del sector de *cloud computing* en materia de seguridad, técnica y jurídica, y transparencia.

b. Recomendaciones del Grupo de Trabajo del artículo 29 para la prestación del servicio del cloud computing.

Parte el Dictamen 05/2012, sobre la computación en nube, con la determinación de la legislación aplicable, conforme a las Directivas de aplicación[181]. Es irrelevante el modelo de implantación del *cloud computing*, más bien habrá que determinar el país donde se establece el responsable del tratamiento, que suele ser, el cliente, independientemente de la nacionalidad de los proveedores o dónde se encuentre el *hardware*. Dentro de las dificultades que plantea emplear la tecnología objeto de estudio, una de las singularidades era conocer en qué momento y lugar se encuentran nuestros datos. Con las instrucciones expuestas en la Directiva, solo se presentarán dudas a la hora de determinar la legislación aplicable cuando el responsable del tratamiento esté establecido en varios Estados miembros y realice la actividad en cada uno de ellos, para lo cual será aplicable la legislación del país en cada uno de los centros donde realice el tratamiento; o en el supuesto de que el responsable del tratamiento no esté establecido en el Espacio Económico Europeo y, sin embargo, realice el tratamiento en el territorio indicado. En

Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

[181] El artículo 4.1.a) de la Directiva 95/46/CE señala que es de aplicación el Derecho nacional de los Estados miembros que adopten la Directiva cuando: *"el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable"*.

este último supuesto será de aplicación el artículo 4.1.c) de la Directiva 95/46/CE[182] y, por tanto, será de aplicación la ley nacional del proveedor del servicio situado en la Comunidad, salvo que *"dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea"*. Por lo tanto, lo primordial será determinar cuándo proveedor y cliente actúan como responsable o encargado del tratamiento en la computación en la nube, dado que delimitará la responsabilidad y las funciones correspondiente de cada parte. Es aquí donde incide el Grupo de Trabajo.

El Dictamen 1/2010 aborda los conceptos de «responsable del tratamiento» y «encargado del tratamiento»[183], adoptado el 16 de febrero de 2010. El Grupo de Trabajo considera que *"el papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica. En otras palabras, debe asignar la responsabilidad"*[184]. Para la correcta delimitación entre ambas figuras establece que *"para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de este"*[185], recalcando que *"el elemento más importante es el que establece que el encargado del tratamiento actúa «por cuenta*

[182] Con la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, deberá atenderse al artículo 2 y, principalmente, al artículo 3 que regula el ámbito de aplicación material y ámbito territorial, respectivamente. Directamente aplicable, a partir del 25 de mayo de 2018, al tratamiento de datos personales de residentes en la Unión *"por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión"*.

[183] Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf . Último acceso: 08.08.2018.

[184] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"", adoptado el 16.02.2010, 2010, 00264/10/ES WP169, p. 4.

[185] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"", adoptado el 16.02.2010, 2010, 00264/10/ES WP169, p. 27.

del responsable del tratamiento». Actuar en nombre de alguien significa servir los intereses de otro y remite al concepto legal de «delegación»"[186].

En la computación en la nube habrá que determinar las actuaciones del cliente y del proveedor del *cloud*. De forma general, será el cliente la parte que decida sobre la finalidad del tratamiento de los datos personales y la responsabilidad asignada, en todo o en parte, de las actividades del tratamiento. El principal objetivo de delimitar los fines del tratamiento es que los usuarios sepan cómo y con qué fines sus datos serán tratados, y con ello puedan determinar si desean confiar en el responsable del tratamiento de los datos. Esta definición *ex ante* excluye la posibilidad de introducir cambios posteriores en las condiciones esenciales del tratamiento. Por el contrario, el suministrador del servicio pondrá a disposición del cliente la plataforma, el medio y el *hardware* habilitados al efecto, actuando en nombre de aquel[187].

A pesar de que habrá que atender a la contratación efectuada, nos recalca el Grupo de Trabajo que la actual evolución de la industria limita las posibilidades que tiene el cliente de negociar las condiciones de uso, al normalizarse las ofertas de la mayoría de los servicios de la nube, por lo que la función estándar del proveedor será la de contratista frente al cliente y, por tanto, encargado del tratamiento[188]. En este marco, se aprecia el esfuerzo realizado por el *Cloud Select Industry Group*[189] en materia de protección de

[186] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"", adoptado el 16.02.2010, 2010, 00264/10/ES WP169, p. 28.

[187] Aunque se abordará en posteriores Capítulos, en materia de protección de datos el artículo 3.2 párrafo segundo de la Directiva 95/46/CE y, para el caso español, el artículo 2.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece la denominada "exención doméstica", por el cuál no será de aplicación las disposiciones recogidas en los citados textos jurídicos cuando el tratamiento de datos personales sea efectuado por una persona física en el ejercicio de las actividades exclusivamente personales o domésticas. Por lo tanto, debe atenderse a la personalidad del cliente y la finalidad con la que emplea el uso de la computación en la nube para ver la aplicación de régimen que ahora se estudia. La exención en el ejercicio de actividades domésticas se replica en el artículo 2.2.c del vigente RGPD. A efectos de estudio, se obviará la exención indicada.

[188] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 5/2012 sobre la computación en la nube", adoptado el 01.07.2012, 2012, 01037/12/ES WP196, p. 10.

[189] El C-SIG es un grupo de trabajo compuesto por representantes de las principales empresas y organizaciones europeas e internacionales que desarrollan servicios de computación en la nube, con la finalidad de realizar propuestas y asesoramientos en pos de un mayor desarrollo del servicio. El grupo se desarrolla en el marco del The European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT). Se puede tener una información más extensa del C-SIG en:

datos al elaborar el *Code of Conduct*, en fase de borrador, analizado por el Grupo de Trabajo en el Dictamen 02/2015, de 22 de septiembre 2015, titulado "*on C-SIG Code of Conduct on Cloud Computing"*[190]. Como nos recuerda el Grupo de Trabajo, *"el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos"*[191]. Serán los proveedores del servicio de la nube, como encargados del tratamiento, quienes lleven a cabo las medidas oportunas sobre seguridad, principalmente, debiendo asesorar y asistir a los clientes en las obligaciones que la normativa les exige a los responsables del tratamiento de datos. Por ejemplo, las herramientas de encriptado y restricción de acceso pueden salvaguardar las exigencias propias del responsable y del encargado del tratamiento.

La prestación del servicio de la computación en la nube se ha desarrollado, en gran medida, por la subcontratación de servicios por parte de los proveedores. Esta cadena de prestadores de servicios conlleva a que personas ajenas a la primitiva relación contractual accedan al tratamiento de datos[192] debiendo todas ellas ajustarse a las exigencias derivadas de las directrices del cliente como responsable del tratamiento de datos. El Grupo de Trabajo se ha manifestado al respecto, indicando que, en su opinión, *"el encargado del tratamiento podrá subcontratar sus actividades únicamente sobre la base del conocimiento del responsable del tratamiento, que suele darse al inicio del servicio, con la inequívoca obligación para el encargado de informar al responsable sobre cualquier cambio previsto en lo que respecta a la adición o sustitución de subcontratistas,*

---

https://ec.europa.eu/digital-single-market/en/cloud-computing-strategy-working-groups. Último acceso: 08.08.2018.

[190] Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf. Último acceso: 08.08.2018. En él se hace un estudio profundo del borrador presentado por el C-SIG sobre el Código de adhesión de la industria de la computación de la nube en materia de protección de datos. A los efectos de nuestro estudio, nos vamos a centrar en las recomendaciones expuestas por el Grupo de Trabajo del artículo 29, sin entrar en el detalle del contenido del Código de conducta.

[191] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"", adoptado el 16.02.2010, 2010, 00264/10/ES WP169, p. 29.

[192] Nos remitimos al Capítulo I, cuando se analizaron los riesgos, la evolución y el actual desarrollo de la computación en la nube, y al Capítulo IV.b.b. que estudia de forma holística la subcontratación en la prestación de servicios de *cloud computing*.

teniendo el responsable del tratamiento en todo momento la posibilidad de oponerse"[193]. Por lo tanto, el cliente debería actuar conforme a las cláusulas de incumplimiento contractual por los daños causados y hacer efectiva las obligaciones entre partes. En este sentido, el reciente Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[194], RGPD, se hace eco de las aportaciones del Grupo de Trabajo, estableciendo en el artículo 28.2 que *"el encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios"*. Aportación especialmente relevante, aunque se restrinja a los datos personales, porque, como veremos en próximos capítulos, los prestadores de servicios de *cloud* suelen subcontratar servicios sin que el cliente tenga conocimiento exacto de la identidad de los subproveedores.

Un nuevo reto, como se resalta en el Dictamen 8/2014 sobre la evolución reciente de la Internet de los Objetos, adoptado el 16 de septiembre[195], será analizar las posibles sinergias y convergencias que pudieran existir entre el desarrollo tecnológico de la computación en la nube y el Internet de las Cosas, IoT (o Internet de los Objetos, como lo define el Grupo de Trabajo)[196].

Para el correcto tratamiento de los datos personales, ámbito de estudio del Grupo de Trabajo del artículo 29, debe garantizarse, en todo momento, que se cumpla el principio de especificación del objetivo y limitación de la finalidad de la obtención y tratamiento de los datos personales, llegando a la destrucción y eliminación de los mismos, de manera segura, cuando decaiga el objetivo y finalidad por la que se recabaron.

---

[193] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 5/2012 sobre la computación en la nube", adoptado el 01.07.2012, 2012, 01037/12/ES WP196, p. 12.

[194] Accesible en:http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES o https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807. Último acceso: 08.08.2018.

[195] Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf. Último acceso: 08.08.2018.

[196] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos", adoptado el 16.09.2014, 2014, 1471/14/ES WP223, p. 6.

Por lo tanto, transparencia, especificación y limitación de la finalidad y supresión de datos son aspectos esenciales para la contratación del servicio. Ya hemos resaltado que en los dictámenes del Grupo de Trabajo se incide que debe ser el cliente quien facilite a los destinatarios o interesados una información amplia sobre la identidad y finalidad del tratamiento, debiendo incluir los encargados y subencargados, si los hubiere, del tratamiento de datos. Esta garantía de transparencia, para la computación en la nube y la amplia cadena entre encargados y subencargados del tratamiento que pueden existir, debe ser exigible por parte del cliente al proveedor y debe ser obligatoria para el cliente en pos de los interesados. Sería, por tanto, recomendable que en el contrato de *cloud* se incluyan medidas técnicas y organizativas, así como auditorías sobre los servicios, que reduzcan el riesgo de que proveedores y subproveedores traten los datos con una finalidad distinta, o incluso para su propio interés, de los que declara el cliente. En el Dictamen 5/2012 sobre la computación en la nube, el Grupo de Trabajo incide en que para la correcta aplicación del principio el cliente debe tener acceso y conocimiento de todos los subcontratistas que operan, así como sus centros de trabajo. De otra forma sería una ardua labor, si no imposible, evaluar el nivel adecuado de protección. Incluso si el proveedor requiere la instalación de programas en el *hardware* del cliente debería informar las implicaciones sobre la actuación[197].

Debe el cliente ser diligente en la selección del proveedor del servicio de computación en la nube para que se garantice que, en la ejecución del contrato, así como finalizado el servicio, se supriman los datos personales decaído el fin que perseguía su tratamiento, en nada influye que el almacenamiento no se produzca en soportes físicos del cliente. Es plenamente aplicable al entorno de la nube el principio de minimización de datos, fundamental en el Derecho de protección de datos, según el cual los datos que no son necesarios para prestar el servicio contratado, como mínimo, deben ser anónimos. El RGPD se hace eco de esta exigencia estableciendo en el Considerando 81 que, finalizado el tratamiento, debe, a elección del cliente, devolver o suprimir los datos personales. Esta obligación se reproduce en el artículo 28.3.g, entre las cláusulas que regirán el contrato entre encargado y responsable del tratamiento Si bien, las diferentes implantaciones del *cloud* pueden dificultar, como señala el Dictamen 8/2014, el flujo de datos generados al

[197] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 5/2012 sobre la computación en la nube", adoptado el 01.07.2012, 2012, 01037/12/ES WP196, p. 13.

no poder revisar el cliente adecuadamente los datos antes de su publicación, lo que genera el riesgo de falta de control y excesiva exposición del usuario[198], teniendo como resultado que el usuario y el cliente puedan no ser consciente del tratamiento de datos.

Defendemos que debe ser el contrato del *cloud computing* quien garantice y regule las relaciones entre el proveedor del servicio y el cliente (encargado y responsable del tratamiento, en principio, respectivamente). Esta sintonía, que se establece como obligatoria en el artículo 28.3 del RGPD, trae causa del artículo 17.3 de la Directiva 95/46/CE, que reseña la obligatoriedad de establecer un contrato formal.

El Grupo de Trabajo, en el Dictamen 5/2012 sobre la computación en la nube, recomienda una serie de cláusulas que debe recoger el contrato del servicio, siempre con la premisa de seguir las instrucciones del responsable, sobre todo en referencia a los niveles de servicios exigibles, medidos de manera objetiva[199]. A estas alturas, conviene decir, que un cumplimiento pulcro de la normativa vigente en materia de protección de datos no es condición suficiente para garantizar un correcto desarrollo de la relación entre cliente y proveedor de la nube. El Grupo de Trabajo, en el Dictamen 02/2015, aclara que adherirse a un código de conducta, aunque sea auspiciado y revisado por el propio Grupo, no exime adaptarse a los cambios de legislación en la materia, si bien, supone una transición suave hacia el marco regulatorio. Insiste que, la adscripción a un determinado código de conducta no garantiza ninguna protección automática contra intervenciones o acciones de las autoridades competentes en la protección de los datos personales[200].

Las medidas técnicas y organizativas del proveedor de la nube deben garantizar la protección de datos y la seguridad del servicio. Por lo tanto, el primer paso será delimitar los posibles riesgos y la naturaleza de los datos a tratar. Es vital, para el responsable del tratamiento, seleccionar un proveedor de servicios que establezca las medidas de seguridad técnicas y de organización adecuadas, y controlar que dichas medidas se

[198] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos", adoptado el 16.09.2014, 2014, 1471/14/ES WP223, p. 8.

[199] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 5/2012 sobre la computación en la nube", adoptado el 01.07.2012, 2012, 01037/12/ES WP196, p. 15-19.

[200] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", adoptado el 22.09.2015, 2015, 2588/15/EN WP232, p. 4-5.

cumplan.[201] La disponibilidad de los datos personales exige determinar, sobre todo en el ámbito de la nube, que el encargado del tratamiento adopte las medidas necesarias para prevenir, o corregir, la pérdida de enlace con el servicio del *cloud*, los ataques malintencionados o los fallos relacionados con terceros ajenos al servicio. Puertas de enlaces, *proxies*, copias de seguridad automática o réplica de servidores que prestan los servicios pueden ser medidas a desarrollar en el contrato.

La disponibilidad está estrictamente vinculada a que los datos no hayan sido manipulados, ya sea de forma malintencionada o accidental. Esta autenticidad puede ser controlada en el entorno de la nube a través de los sistemas de prevención y detección de intrusiones (IPS/IDS). En esta relación contractual, debe ser el proveedor quien proporcione al cliente un nivel de detalle suficiente sobre las medidas de seguridad implementadas, según el modelo y las especificidades del servicio, así como del nivel de transformación y la naturaleza de los datos, para que el cliente pueda conocer las vulnerabilidades y, de esta forma, gestione las decisiones en función de sus instrucciones[202].

La técnica del cifrado de datos en tránsito y en reposo, así como las propias relaciones en el seno de la prestación del servicio entre el cliente y el encargado, posibilitan, o al menos suponen una salvaguarda, la confidencialidad de los datos personales. Claves criptográficas, medidas de autentificación y autorización, registros de acceso vinculados a usuarios, entre otras, llevadas a cabo por el proveedor son medidas que definen técnicas apropiadas para un correcto desarrollo de la computación. Dependerá del servicio contratado para que estas medidas, aunque no excluyentes, pero sí determinantes, se garanticen antes, mientras o después de trasladar los datos a la nube.

Para la contratación de la nube, el objeto y el alcance del servicio deben estar delimitados y desarrollados de forma clara. Aunque serán los Acuerdos de Nivel de Servicio los que complementen, en gran parte, estas cláusulas contractuales, a los efectos de protección de datos interesa reseñar de forma expresa el alcance, la finalidad y la forma en que el cliente y encargado del tratamiento gestionan la obtención de datos.

---

[201] En el Capítulo IV.b. veremos como el RGPD responsabiliza al cliente de la correcta elección del proveedor de servicios.

[202] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", adoptado el 22.09.2015, 2015, 2588/15/EN WP232, p. 10-11.

El soporte físico, salvo en redes privadas, es compartido por diferentes clientes. Establecer medidas que aíslen los datos trasladados a la nube, con el fin de garantizar la confidencialidad, integridad y finalidad con la que se utilizan los datos es de obligado cumplimiento. Las restricciones en el acceso a los datos, ya citados, para las finalidades y usuarios correspondientes, deben combinarse con cláusulas de confidencialidad entre las partes del contrato, extendiendo esa obligación al personal dependiente del proveedor y al posible subencargado del tratamiento. Junto con la cláusula específica que obligue al proveedor a no comunicar datos a terceros, se deberá recoger, si así se estima y para garantizar el control del cliente como responsable del tratamiento, que será necesaria previa autorización para contratar subencargados del tratamiento[203]. La posibilidad de oponerse a la subcontratación o de rescindir el contrato con el proveedor, y la opción de conocer las relaciones establecidas entre el proveedor de la nube y los posibles subencargados posibilitan al cliente evaluar riesgos y, al menos, garantizar que se sigan las instrucciones dadas, como responsable del tratamiento.

Será el cliente el responsable de garantizar que los usuarios puedan ejercer sus derechos de acceso, rectificación, supresión, bloqueo y omisión. Sin embargo, es interesante que en el contrato del *cloud computing* se recoja que el proveedor, que posiblemente disponga de los medios técnicos oportunos, apoye al cliente en la obligación indicada. Es oportuno, además, establecer los estándares que utilizará el proveedor del servicio, principalmente en formato e interfaces normalizados o abiertos, para evitar y mitigar los costes *lock-out* y, en consecuencia, *lock-in*, y hacer portables los datos.

Con todas las premisas anteriores, delimitar la responsabilidad de las partes del contrato, clasificándolas, determinará quién asume las medidas adecuadas para garantizar la protección de datos personales. Solo a partir de esta delimitación expresa se podrá exigir al cliente y al proveedor la adopción de medidas técnicas oportunas y efectivas dentro de su ámbito de actuación. El Grupo de Trabajo considera que es necesario recoger de forma fehaciente las áreas en las que cliente y proveedor actúan como controlador o

[203] Ya se ha indicado la obligatoriedad que recoge el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

procesador, para una correcta asignación de la responsabilidad entre las partes[204]. Sería pertinente que, además de delimitar las responsabilidades y las actuaciones de las partes, se lleve a cabo la notificación a la contraparte del acceso, utilización o violación de los datos objeto de tratamiento.

Decíamos en el Capítulo I que una de las características del servicio de computación en la nube es la deslocalización, es decir, la desubicación estable de los datos que se trasladan a la nube. En el Dictamen 02/2015 se recomienda que los proveedores contribuyan a la correcta localización donde se realiza el procesamiento, para que con ello se permita al controlador identificar las leyes aplicables, más cuando está fuera del espacio EEE[205]. Incluso, las leyes nacionales de referencia de algunos Estados Miembros exigen al controlador supervisar de forma activa, monitorizar e inspeccionar las medidas de seguridad del tratamiento. El Grupo de Trabajo, consciente de ello, recomienda que en el contrato del servicio se recoja la obligación del proveedor de proporcionar la lista de lugares donde se tratarán los datos. Las transferencias internacionales de datos encuentran su encaje legal en el RGPD[206], si bien fuera del EEE requiere garantizar el nivel de protección adecuado. El Grupo de Trabajo reconoce que el entorno de la nube dificulta unas comprobaciones sólidas sobre el nivel adecuado de protección de los proveedores en terceros países, de ahí que considere insuficiente la autocertificación con puerto seguro como *conditio sine qua non* de garantía de protección de datos. En este sentido, junto a las pruebas de existencia de autocertificaciones de puerto seguro se deben requerir pruebas fehacientes de que se cumple dicho principio. Es común en la contratación de la computación en la nube que el proveedor del servicio no ofrezca los requisitos que la legislación nacional le exige para operar, sin embargo, dentro de la diligencia del cliente

[204] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", adoptado el 22.09.2015, 2015, 2588/15/EN WP232, p. 9.

[205] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", adoptado el 22.09.2015, 2015, 2588/15/EN WP232, p. 7.

[206] En el Capítulo IV.b.c. analizaremos de manera detallada el alcance de las transferencias internacionales de datos a la luz del RGPD y, en aquello no regulado y siempre que no entre en contradicción, con la LOPD y el RLOPD.

se debe evaluar que los contratos tipos celebrados con los encargados o subencargados de tratamiento reúnen las premisas necesarias[207].

Advierte el Grupo de Trabajo que los principios de puerto seguro no garantizan las medidas de seguridad apropiadas en los Estados Unidos, el exportador podría perder la gobernanza de los datos, no asegurarse un correcto aislamiento de datos o, entre otros, no tener una garantía sobre la auditoría técnica del proceso. Debe ser el cliente quien realice una labor de comprobación[208].

En el análisis del borrador del Código de conducta del C-SIG se recomienda obligar al proveedor a comunicar al cliente cualquier solicitud legalmente vinculante para la divulgación de los datos personales por un servicio de seguridad, a menos que esté prohibido, garantizando que, en cualquier caso, la transferencia a la autoridad pública no sea masiva, desproporcionada o indiscriminada[209]. Recordar que cuando el proveedor del servicio actúa fuera de las propias instrucciones del cliente será considerado responsable del tratamiento de datos.

c. Experiencias internacionales

En la actualidad no hay ningún régimen jurídico que proporcione una regulación completa de la herramienta del *cloud computing*, si bien, diferentes gobiernos estatales han intentado, al menos, marcar las directrices del desarrollo del servicio, sobre todo cuando la contratación de la nube influye directamente en la Administración pública. Estados Unidos, Reino Unido, México, Colombia o Canadá se han hecho acopio de la nueva tecnología a través de una estrategia definida[210].

---

[207] No hay que olvidar que el artículo 28.3 del RGPD exige la firma del contrato o acto jurídico entre el responsable de datos, que suele ser el cliente, y el encargado de datos, proveedor de servicios de la nube.

[208] Las excepciones que se recogen en el Documento de Trabajo 12/1998, de 24 de julio de 1998, sobre Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, no son aplicables al no producirse la urgencia, el procedimiento es sistematizado, el tratamiento de datos es de forma completa y es frecuente la relación en el servicio, además de ser una disposición derogada. El tratamiento completo de las excepciones se realiza en las páginas 26-27. Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf. Último acceso: 08.08.2018.

[209] ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", adoptado el 22.09.2015, 2015, 2588/15/EN WP232, p. 8.

[210] En este contexto, hay proyectos, como la nube soberana de Francia, denominada Andromède, que han fracasado por la dificultad de consensuar posiciones entre proveedores y Gobierno. Para más información, CUNY, Delphine: "Le cloud à la française, histoire d'un flop ?", *LaTribune.fr* , 2015 (13.01.2015).

Vamos a resaltar la experiencia del *cloud* en Estados Unidos, al ser el primer gobierno que ha tratado una regulación del fenómeno; la implantación en Reino Unido, al poseer el marco reglamentario, a nuestro parecer, más completo sobre la tecnología y su incidencia; y la incipiente aparición de la normativa de la nube en Canadá, que se encuentra en proceso de formulación y nos servirá para determinar si existe un cambio estratégico dentro de la regulación de nuestro objeto de estudio[211].

Rasgo común de todas las iniciativas para iniciar la migración es el estudio completo de los riesgos a los que se enfrenta el órgano de contratación, analizando las posibilidades de mitigar los riesgos de seguridad y los controles y salvaguardas ante intrusos, la indisponibilidad del servicio, el robo de información o inoperatividad de la nube, entre otras incidencias, que se pueden producir en el desarrollo de la actividad administrativa. Serán, por tanto, los datos considerados confidenciales los menos propensos a trasladarlos a la nube o, directamente, no recomendados a "externalizar" (nube pública) o permitir la posibilidad de un uso compartido. Serán en última instancia los responsables gubernamentales, apoyados por el equipo técnico, los que decidan mantener la información en infraestructuras *on-premise*, trasladarla a nubes privadas, híbridas o públicas. VALLE (Microsoft)[212], aunque no es un sistema de clasificación que siguen todos los países que han regulado la tecnología, establece cinco niveles de segmentación de datos en función de la información de la que disponen las Administraciones públicas:

- Nivel 1: Información confidencial, como la referente a la seguridad nacional o económica del país.
- Nivel 2: Información restringida y solo compartida con algunos funcionarios.
- Nivel 3: Información utilizada dentro del funcionariado, como podría ser la relativa a los trámites y servicios, que no contiene datos personales ni sensibles.

Accesible en: http://www.latribune.fr/technos-medias/informatique/20150113triba29598d73/le-cloud-a-la-francaise-histoire-d-un-flop.html. Último acceso: 08.08.2018.

[211] Aunque se ha centrado el estudio en tres propuestas de programas de la nube, por la importancia que tienen en el sector y para mostrar la evolución y enfoques en la regulación, se recomienda un análisis del *Trusted Cloud*, programa presentado por el Ministerio de Economía y Energía de la República Federal de Alemania. Información accesible (complementaria) en: http://www.digitale-technologien.de/DT/Navigation/EN/Ueber_Uns/ueber_uns.html y, sobre todo, en la web principal de *Trusted Cloud*, https://www.trusted-cloud.de/cloud-service-suche. Últimos accesos: 08.08.2018.

[212] VALLE, Teresa: "Los gobiernos pueden migrar a la nube con confianza", *New Center Latinoamérica*, Microsoft, 2016 (28.01.2016). Accesible en: http://news.microsoft.com/es-xl/features/los-gobiernos-pueden-migrar-a-la-nube-con-confianza. Último acceso: 08.08.2018.

- Nivel 4: Información anónima que solo puede ser visualizada, principalmente, para su análisis público.
- Nivel 5: Datos públicos al alcance de los ciudadanos, como por ejemplo la información sobre el clima.

A partir de esta clasificación, VALLE establece un tipo de implementación de la nube distinto para las instituciones públicas en función de la información a trasladar al servicio. Sin embargo, en una sociedad que exige a sus gobernantes una mayor transparencia, como principio rector del proceso político y de la actividad gubernativa, y en mayor medida administrativa e institucional, sería oportuno aunar los niveles 3, 4 y 5 en uno solo, como ha realizado Reino Unido, al no contener información de carácter personal o que pudieran contravenir los altos intereses del Estado. Esta clasificación, realizada de forma interesada para el sector público, en sentido amplio, es perfectamente extrapolable al sector privado. Si en un futuro, poco probable, los Estados tienden a una regulación del servicio, que al menos sirva de prácticas de uso, para el sector privado, sería perfectamente extrapolable a las empresas, adaptándola a la relevancia de la información clasificada. No puede perderse de vista que esta categorización intenta disuadir el óbice de la migración a la nube y las fallas de seguridad.

a. Primeros pasos: FedRAMP de EEUU

FedRAMP, acrónimo de *Federal Risk and Authorization Management Program*[213], es un programa impulsado por la administración de EE.UU. que pretende evaluar los servicios y productos del *cloud computing*. Antes de aparecer el programa, cada agencia gubernamental gestionaba de forma individual sus propias metodologías de evaluación.

Se autodefine como un "programa para la administración que proporciona un enfoque estandarizado de evaluación de la seguridad, monitoreo, autorización y supervisión continua de los productos o servicios de la nube"[214]. Tras el documento *"Federal Cloud*

[213] Web oficial de FedRAMP: https://www.fedramp.gov/. Último acceso: 08.08.2018.

[214] Traducción libre del original: *"The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services"*. Extraído de https://www.fedramp.gov/about/. Último acceso: 08.08.2018.

computing strategy"[215] presentado por Vivek Kundra, *U.S. Chief Information Officer*, el 8 febrero de 2011, y, sobre todo, el "*Memorandum for Chief Information Officers"*, firmado por Steven VanRoekel, Federal *Chief Information Officer*, sobre "las autorizaciones de seguridad en los sistemas de información bajo el entorno de la computación en la nube"[216], de 8 de diciembre de 2011[217], el FedRAMP ha sometido a los proveedores de servicios de la nube, que quieran operar con el aparato institucional de EE.UU., a la auditoría y evaluación de una organización externa, denominada en el programa 3PAO, para garantizar que el servicio ofrece los sistemas de seguridad y las autorizaciones establecida por la Ley Federal de Seguridad de Información (FISMA)[218]. Con una evaluación de los mecanismos, procesos e instrumentos de seguridad del proveedor se puede extender el servicio al amplio abanico gubernamental de EE.UU.

A modo de introducción, el proceso de autorización de FedRAMP se basa en tres pasos: evaluación de seguridad, a través del conjunto estandarizado de requisitos que determina la FISMA; el proceso de autorización de las agencias federales, tras los procesos de autorización de seguridad y repositorio del FedRAMP; y la evaluación continua de seguridad y autorización, con el fin de mantener la seguridad.

Para conocer la relevancia del FedRAMP dentro de la administración puede ser clarividente ver la composición de las entidades que la conforman. A saber, la Oficina de Gestión y Presupuestos (OMB), la Administración de Servicios Generales (GSA), el Departamento de Seguridad Interna (DHS), el Departamento de Defensa (DOD), el Instituto Nacional de Estándares y Tecnología (NIST) y el Consejo General de los Directores de Informática (CIO Council). Es la Junta de Autorización Conjunta o Junta

---

[215] Accesible en: https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf. Último acceso: 08.08.2018.

[216] Originariamente titulado *"Security Authorization of Information Systems in Cloud Computing Environments"*. Accesible en: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/fedrampmemo.pdf. Último acceso: 08.08.2018.

[217] La capacidad operativa inicial del FedRAMP nace el 6 de junio 2012, si bien no es hasta el 5 de junio de 2014 cuando el servicio de la FedRAMP se vuelve operacional, debiendo reunir los requisitos de seguridad prescritos en todas las autorizaciones en la fecha indicada, para la contratación de la nube en los entes obligados.

[218] La última modificación de la *"Federal Information Security Modernization Act"* data de 18 de diciembre de 2014. Accesible en: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf. Último acceso: 08.08.2018.

Mixta de Autorización (JAB) el órgano principal de gobierno del FedRAMP, compuesto por representantes del GSA, DOD, y los directores de informática del DHS. Este conglomerado de entes públicos, que encarnan la defensa, la seguridad y la viabilidad del Estado, requiere de la estrecha colaboración de los expertos en seguridad cibernética, sobre todo de la nube, y de la industria privada para su correcto funcionamiento.

La importancia del FedRAMP, haciendo acopio de la exposición del proveedor evaluado Amazon Web Service[219], aumenta por:

- *"La uniformidad y la confianza en la seguridad de las soluciones en la nube que utilizan NIST y las normas definidas en la ley FISMA*
- *La transparencia entre el gobierno de EE.UU. y los proveedores en la nube*
- *La automatización y una monitorización continua casi en tiempo real*
- *La adopción de soluciones en la nube seguras a través de la reutilización de evaluaciones y autorizaciones."*

A estos beneficios y metas, recogidos de forma similar en el memorándum del FedRAMP, hay que añadir la búsqueda para asegurar la aplicación coherente de las mejores prácticas de seguridad existentes, ahorro de costes, recursos y tiempos en evaluar los distintos servicios, el fomento de un conjunto básico de normas acordadas y el respaldo y confianza en las evaluaciones de seguridad como método para prevenir y evaluar los riesgos que conlleva la implantación del *cloud computing*.

Tres son las vías para que los proveedores puedan alcanzar el reconocimiento de la FedRAMP[220]:

- Autorización provisional de la Junta de Autorización Conjunta (JAB). Los proveedores de la nube son inspeccionados por la oficina de gestión de proyectos (PMO) de la FedRAMP, son evaluados de forma externa por un 3PAO acreditado y reciben una autorización provisional para operar (P-ATO), tras la conformidad de los directores de información de DHS, DOD y GSA.
- Autorización a través de una agencia del FedRAMP. En este supuesto, los proveedores de los servicios de la nube presentan la documentación

[219] Extracto de https://aws.amazon.com/es/compliance/fedramp/. Último acceso: 08.08.2018.

[220] El desarrollo completo se encuentra en el documento *"Guide to Understanding FedRAMP"*. Accesible en: https://www.gsa.gov/cdnstatic/Guide_to_Understanding_FedRAMP_042213.pdf. Último acceso: 08.08.2018.

correspondiente, para su inspección, al Director de información o delegado autorizado de una de las entidades que componen el FedRAMP. Evaluada y verificada la documentación conforme a los criterios predefinidos, recibe una autorización de funcionamiento (ATO) por parte del PMO del FedRAMP. La ATO obtenida para el uso del servicio reduce los costos y tiempo de esperas para extrapolar el servicio a otra agencia.

- Evaluación de seguridad completa por el PMO del FedRAMP. Los proveedores de la nube que elijan esta ruta entregan la documentación completa prescrita por el FedRAMP para el estudio de seguridad completa por el PMO del FedRAMP, provista de la evaluación de una 3PAO acreditada por el FedRAMP. Toda la documentación y las evaluaciones del 3PAO, completas, están disponibles para la revisión de las agencias que quieran contratar el servicio, por lo tanto, aunque no suponga una autorización (P-ATO o ATO) disminuye el tiempo para sus aprobaciones.

Con estos tres procesos se pretende acelerar los métodos de elección, evaluada la seguridad y los procesos de monitorización del servicio, de la adopción de la nube por las agencias gubernamentales. Una vez obtenida la autorización P-ATO o ATO se puede utilizar el servicio con la garantía de que:

- Los servicios han sido creados con paquetes de seguridad predefinidos por el FedRAMP.
- Los sistemas cumplen con los requisitos de control de seguridad de la FedRAMP.
- El servicio ha sido evaluado por una entidad independiente y externa a las organizaciones contratantes, 3PAO.
- Con las autorizaciones P-ATO y ATO o la carta de autorización archivada en el sistema tras la evaluación del PMO FedRAMP se certifica el servicio de los proveedores.

En resumen, para poder operar conforme a los requisitos preestablecidos por el FedRAMP, el proveedor de la nube debe contar con la preceptiva autorización para contratar con los órganos gubernamentales federales, el servicio que ofrece el proveedor debe respetar los controles de seguridad que establece FedRAMP y que están en conexión

con las normas NIST 800-53 rev.4[221], todos los sistemas de seguridad deben desarrollarse a través de las plantillas que exige la FedRAMP, todos los servicios tienen que estar evaluados por un auditor independiente, y deben publicarse las evaluaciones de seguridad en el repositorio del FedRAMP. El proceso de autorización debe completarse por todos los proveedores de la nube, sean entidades comerciales o gubernamentales.

En el *MarketPlace*[222] de la web oficial del FedRAMP podemos encontrar los proveedores autorizados o en proceso de autorización, con indicación de su estado, el servicio de la nube autorizado y el nivel de impacto. Además, existe la posibilidad de discriminar entre agencias y productos autorizados.

La implantación del FedRAMP supone un avance importante en la regulación del *cloud computing*, propiciado por los agentes que disfrutaran del servicio. Aunque claramente es un programa destinado para las Administraciones públicas federales de EE.UU., el sector privado puede valerse de las autorizaciones y evaluaciones realizadas para implantar un servicio que goce con las mismas premisas que para el aparato gubernamental. Sin embargo, como crítica, no queda otra que resaltar como el programa se centra solo en uno de los riesgos que supone la migración a la nube, la seguridad. Todo el programa gira en mejorar las grietas, vulnerabilidades, deficiencias y costes que supondría que terceros ajenos al servicio pudieran acceder a la información o que el servicio se encuentre inoperativo. Probablemente, por los sujetos que se benefician del programa, grandes agencias federales de EE.UU., el poder negociador en la contratación de los servicios de la nube sea equilibrado, pudiendo incluir las cláusulas contractuales favorables al cliente que regirán el devenir de la contratación del *cloud computing*. Empero frustra un verdadero marco jurídico y técnico que rija la tecnología objeto de estudio, no solo para el sector público en general, del que podrían beneficiarse administraciones menores del conglomerado de Estados, sino el sector privado, que podrían tener un marco de referencia para regular el servicio.

[221] Accesible en: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Último acceso: 08.08.2018.

[222] Accesible en: https://marketplace.fedramp.gov/index.html. Último acceso: 08.08.2018.

b. UK Government G-Cloud, una propuesta de Acuerdos Marcos para la computación en la nube en la Administración pública de Reino Unido.

UK Government G-Cloud[223], más conocido como G-Cloud, se configura como un programa para la contratación de los servicios de la nube para la Administración pública de Reino Unido, que a iniciativa del Gobierno pretende ser la herramienta aplicable a todos los departamentos gubernamentales. La novedad que presenta la iniciativa radica en la epistemología del G-Cloud. Microsoft[224], en la definición del servicio, resalta la idiosincrasia del programa: *"G-Cloud comprises a series of framework agreements with cloud services suppliers (such as Microsoft), and a listing of their services in an online store—the Digital Marketplace. This enables public-sector organizations to compare and procure those services without having to do their own full review process"*. Acuerdos marcos con proveedores del servicio, tienda en línea, revisión completa y amplitud para adherirse a todas las instituciones de carácter público son las señas de identidad de la iniciativa y lo que diferencia al programa de otras experiencias internacionales, como el estudiado FedRAMP.

En octubre de 2011, el Gobierno publica *"Government Cloud Strategy"*[225] que recoge la estrategia sobre la computación en la nube del Gobierno de Reino Unido. Con esta medida el Gobierno intenta explotar los beneficios que esta herramienta genera en pos de mayor productividad de los recursos humanos, mayor flexibilidad y rentabilidad. La innovación supone un cambio radical en los procesos actuales[226], lanzándose el servicio en 2012 como "un programa continuo e interactivo que permitirá el uso de una amplia gama de servicios en la nube, atendiendo a los cambios que operan en la nube, para su

[223] La web oficial de G-Cloud: https://www.digitalmarketplace.service.gov.uk/. Último acceso: 08.08.2018.

[224] Extracto de: https://www.microsoft.com/en-us/TrustCenter/Compliance/UK-G-Cloud. Último acceso: 08.08.2018.

[225] "*Government Cloud Strategy"*, documento accesible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf. Último acceso: 08.08.2018.

[226] Se recomienda leer el extracto sobre la sub-estrategias TIC publicado por *Minister for the Cabinet Office* (27.10.2011). Accesible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266204/mco-foreword-ict-sub-strategies.pdf. Último acceso: 08.08.2018.

adquisición en las Administraciones públicas"[227]. De esta forma, las Administraciones públicas tienen el respaldo de un órgano revisor que pretende proporcionar un nivel aceptable de mitigación de riesgos y garantiza el cumplimiento de las obligaciones legales y reglamentarias establecidas para la implantación del servicio. Con este modelo centralizado se pretende, por tanto, una estrategia común de los servicios del *cloud* y su puesta en marcha, un enfoque global en la aprobación y gestión de los servicios tecnológicos, un enfoque de gobernanza inclusiva, y una gestión descentralizada de la responsabilidad en centros especializados.

El programa G-Cloud, del que responden los *CIO Delivery Board*, se articula a través de 14 principios básicos al que deben responder los consumidores del servicio, las Administraciones públicas que contraten el servicio, y los proveedores de la nube. Los primeros evaluarán los criterios esenciales y la garantía en su elección, conforme a sus necesidades propiciado por un consentimiento informado, y los suministradores de los servicios, deberán atender a los condicionantes expuestos para presentar las ofertas adecuadas. Los ítems a los que deben atender, tanto proveedores como consumidores en función de la posición, se resumen en los siguientes[228]:

- Protección de los datos en tránsito, relacionado con la integridad y confidencialidad de los datos en tránsito.
- Protección de activos, en referencia a la protección contra la manipulación física, pérdida o daños.
- Separación entre los consumidores, buscando la confidencialidad e integridad de los datos o servicios entre consumidores.
- Gobernanza del proveedor, materia de la gestión global del servicio y la información por parte del suministrador del servicio, gestionando y coordinando los riesgos de seguridad potenciales.
- Seguridad operacional, con el fin de impedir, detectar o prevenir ataques contra el ejercicio.

[227] Traducción libre del original: "*G-Cloud is not a single entity; it is an ongoing and iterative programme of work which will enable, the use of a range of cloud services, and changes in the way we procure and operate ICT, throughout the public sector".* Extraído de "*Government Cloud Strategy"*, p. 5.

[228] Puede obtenerse un sumario de los 14 principios de seguridad del programa G-Cloud en *"CESG, the National Technical Authority for Information Security within UK Government"*. Accesible en: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles. Último acceso: 08.08.2018.

- Control del personal que gestiona el servicio, en concordancia con el empleo seguro y la capacitación de los recursos humanos.
- Programa de mejora de la seguridad del servicio.
- Control de seguridad en la subcontratación del servicio o suministrador del proveedor, para garantizar que los principios de seguridad se cumplen.
- Facilitación de un programa de gestión de actuación segura por los consumidores, para que solo las personas autorizadas puedan acceder al servicio y siempre limitada su actuación a la operativa y funcionalidad requerida.
- Identidad y autentificación.
- Protección de la interfaz externa.
- Administración de un servicio seguro en el cual los proveedores de servicio diseñan el acceso operacional para mitigar los riesgos de seguridad en el servicio.
- Auditorías públicas de los servicios de los proveedores.
- Responsabilidad de los consumidores en la utilización del servicio.

Los criterios expuestos, con implicación para los dos sujetos intervinientes en la relación, permiten a los proveedores de servicios auto certificar y suministrar pruebas de apoyo de la seguridad del servicio, y a los consumidores les posibilita tener una visión general del entorno de riesgo y adoptar una decisión informada del servicio de la nube y del proveedor conforme a sus necesidades. Los usuarios, que recordemos pueden ser todos los departamentos gubernamentales de Reino Unido, las Administraciones descentralizadas, las autoridades locales, y en general todas las Instituciones que tengan algún carácter público[229], deben evaluar las necesidades estableciendo una serie de criterios imprescindibles y una lista de características deseables, buscando servicios en el mercado digital, desarrollado por el G-Cloud, y elegir entre aquellos que más se adecúen a sus requerimientos[230].

Una de las características definitorias, diferenciadora de otros programas internacionales, del G-Cloud es la normativización de la relación entre proveedores del

[229] Podemos tener un listado completo de Instituciones elegibles en: https://www.gov.uk/government/publications/public-sector-organisations-eligible-to-use-cloudstore. Último acceso: 08.08.2018.

[230] El Gobierno pone a disposición de las administraciones compradoras una guía de ayuda. Accesible en: https://www.gov.uk/guidance/g-cloud-buyers-guide. Último acceso: 08.08.2018.

servicio y el Gobierno, que será documento base de la reglamentación entre el cliente (administración final contratante) y suministrador, a través de Acuerdos marcos. Estos documentos son acordados entre el Gobierno y los proveedores dividiéndose en 4 categorías según los servicios a contratar para la nube: *IaaS*, *PaaS*, *SaaS* y *SCS*. Este último acrónimo hace referencia a *Cloud Services Specialist*, servicio que apoya la transición a la nube de los clientes.

¿Cuál es el proceso básico de los Acuerdos marco? ¿Qué documentos deben presentar los proveedores? Antes de responder a estas preguntas debemos aclarar que la concertación de Acuerdos marcos solo habilita a los proveedores a ofrecer sus servicios en el *MarketPlace* del G-Cloud, posteriormente clientes (compradores) y proveedores deberán firmar un contrato, denominado *call-off*, que complementará la regulación del servicio contratado.

Para conformar un Acuerdo marco, el Gobierno publica el anuncio de licitación en el Diario Oficial de la Unión Europea (DOUE)[231], momento en el cual los proveedores de la nube pueden presentar la información y documentación requerida para ser estudiada. Analizada la documentación por los responsables del programa, se hace accesible a los compradores para que puedan comparar sus necesidades con los servicios que ofrece el prestador. Entre la documentación a presentar por los proveedores está la aceptación a las condiciones expuestas en el anuncio del Gobierno, proporcionar información básica del proveedor, describir el servicio según los parámetros proporcionados, mostrar la fijación de precios del servicio y los términos y condiciones específicos para el desarrollo del servicio. Es especialmente relevante este último documento, dado que los términos recogidos y las condiciones no pueden ser modificados mientras el Acuerdo marco esté en vigor. Todos los documentos deben estar en formato abierto. Con todo, el *Crown Commercial Service* (CCS), órgano encargado del control de cumplimiento de la información, verifica y evalúa la documentación, asegurando la adecuación con el anuncio marco del Gobierno y si la información y las características del servicio en la

[231] Tras el referéndum sobre el "Brexit", realizado el 24 de junio de 2016, donde los ciudadanos decidieron abandonar la Unión Europea, se han generado dudas, en el ámbito político y jurídico, sobre las implicaciones que tiene la aplicación de la normativa europea, así como los mecanismos que la Unión pone a disposición de los Estados miembros. Corresponde a Reino Unido efectuar las directrices que establece el artículo 50 del Tratado de Lisboa, estableciéndose un plazo máximo de 2 años, desde la notificación de retirada del estado, para dejar de aplicar la reglamentación europea. Hasta la fecha, 08.08.2018, el Gobierno de Reino Unido no ha aclarado el proceder.

nube presentada es consistente. Pasado este control, los servicios estarán disponibles para su compra en el mercado digital. Los Acuerdos marcos de G-Cloud se liberan de 6 a 9 meses, teniendo una duración máxima de 12 meses[232] [233].

Como se ha reseñado anteriormente, los compradores deben suscribir un contrato, *call-off*, con los proveedores de servicios en la nube. Los usuarios accederán al mercado digital habilitado debiendo aceptar los términos y condiciones recogidas, hechas pública, para contratar el servicio. El propio programa limita la duración máxima de los contratos suscritos a 24 meses. Esta limitación temporal tiene como finalidad que las administraciones estén en continua evaluación de las necesidades y requerimientos de sus servicios en la nube. Si surgiera algún tipo de disputa entre la reglamentación contenida en las condiciones impuestas por el proveedor (generales) en el Acuerdo marco y el contrato particular, los términos marcos tendrán prioridad[234].

En el mercado digital, además de los servicios en la nube, se puede contratar o acceder, por un lado, a los resultados y las investigaciones en el entorno digital, y por otro, a la contratación de centros de datos físicos, *hosting*, para los datos que no pueden ser migrados a la nube.

En todo este desarrollo del programa G-Cloud se ha puesto de relieve el avance que supone que un Acuerdo marco recoja términos globales, no solo aspectos relacionados con la seguridad del servicio, aunque sí prominentes, propiciando una regulación mínima (Acuerdos marcos) y contraprestaciones particulares (contratos *call-off*). Sin embargo, los compradores particulares se encuentran muy limitados en su capacidad de negociación de cláusulas, teniendo naturaleza de contrato de adhesión. Por lo tanto, aunque las administraciones contratantes pueden elegir un servicio que se adecúe a sus necesidades,

---

[232] A fecha de 08.08.2018 se encuentra cerrado el *G-Cloud 10 framework* para la licitación de nuevos proveedores en la nube (accesible en: https://ccs-agreements.cabinetoffice.gov.uk/g-cloud-10) si bien los clientes pueden comprar los servicios en base a los programas *G-Cloud 9* (accesible en: https://ccs-agreements.cabinetoffice.gov.uk/contracts), que finaliza en septiembre de 2018. Últimos accesos: 08.08.2018. Es posible la coincidencia de dos *framework*, por la distinta temporalidad de la duración máxima de cada Acuerdo marco (12 meses) y la liberación de cada acuerdo (9 meses).

[233] El Gobierno pone a disposición de los proveedores del servicio una guía de ayuda. Accesible en: https://www.gov.uk/guidance/g-cloud-suppliers-guide. Último acceso: 08.08.2018.

[234] Recomendamos leer cómo proceder, adscribes, con la contratación una vez que se ha seleccionado el servicio: https://www.gov.uk/guidance/how-to-award-a-contract-when-you-buy-services. Último acceso: 08.08.2018.

dado que son públicos todos los términos y condiciones que regirán el servicio, no son personalizados[235]. Aunque el programa está claramente destinado a las instituciones públicas, *ad supra* se detallaban los compradores potenciales, el sector privado puede verse beneficiado de la política desarrollada. En primer lugar, los proveedores de la nube ajustaran su oferta de servicios a los requisitos exigidos en los Acuerdos marcos de las distintas versiones G-Cloud. Es previsible que todas las mejoras en el sector, exigidas en el curso de cada nuevo programa del Gobierno de Reino Unido, se trasladen a la oferta global de los proveedores de la nube. Y, en segundo lugar, al recoger de manera pública los documentos exigidos a los suministradores del servicio para poder formar parte del mercado digital del G-Cloud, los clientes de naturaleza jurídica privada pueden analizar las prestaciones de los proveedores con las necesidades que requieren, pues previsiblemente se reproduzcan, salvo alguna diferenciación como puede ser el precio, en los contratos, principalmente de adhesión, que ofrezcan para la ejecución del servicio[236].

c. Canada Right Cloud, la adopción de la nube solo cuando es necesario[237].

El Gobierno federal de Canadá inicia en noviembre de 2014 una serie de encuentros con la industria de la nube y los entes inferiores de gobierno para consensuar la estrategia general del Gobierno federal respecto a la adopción de soluciones en el entorno del *cloud*

[235] Recomendamos leer el caso de estudio sobre la implantación de la nube a través del programa G-Cloud recogido por JONES. JONES, Steve: "Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study", *International Journal of Information Management*, 2015, Volume 35, Issue 6, p. 712-716.

[236] Para tener una idea general de las posibilidades de investigación o análisis de los aspectos que regirán la relación contractual, se recomienda acceder a algunos de los proveedores y servicios que ofrece el mercado digital de G-Cloud. Por ejemplo, para la contratación de *Intranet Platform Microsoft SharePoint*, de la empresa SFW Ltd, modelo de nube *SaaS*, se recoge la tabla de precios del servicio y su forma de pago, la definición de los servicios, la tarjera SFIA y los términos y condiciones. Accesible en: https://www.digitalmarketplace.service.gov.uk/g-cloud/services/7020015080653651. Último acceso: 08.08.2018.

[237] Antes del desarrollo del siguiente epígrafe queremos advertir que el programa se encuentra en formación. Este hecho limita la capacidad de análisis e investigación, el Gobierno de Canadá aún no ha publicado la configuración completa de la estrategia. Hasta el 30 de septiembre de 2016 existía la posibilidad de plantear comentarios y propuestas entre las distintas instituciones y organismos públicos implicados. Sin embargo, por las innovaciones que va presentando y la posibilidad de analizar, aunque limitada, un programa abierto en la actualidad al debate público se ha considerado necesario hacer esta breve reseña. [Actualización: A fecha de revisión, 08.05.2018, el programa continúa en proceso de formación, no presentando ninguna novedad relevante, al menos pública].

computing[238]. Fruto de este proceso aparece la *Cloud Adoption Strategy*[239]. La novedad que presenta respecto a sus predecesores en el contexto internacional es dar a los directores TI la posibilidad real, en función de las necesidades, de usar o no la tecnología en función del contexto de su organización. Fiel reflejo de esta libertad de adopción de la nube es lo establecido en el apartado "principios para la adopción de la nube":

> *"The GC's Right Cloud adoption strategy recognizes that different deployment and service-delivery models will deliver, to varying extents, the benefits that the GC seeks from Cloud, however CIOs must weigh those benefits against their business requirements".*

El Gobierno de esta forma muestra su preocupación y conciencia de la heterogeneidad de los contornos tecnológicos en sus Instituciones, e incita a una reflexión sobre la adopción de la nube para que la instauración de esta nueva tecnología no sea fruto de una moda o una presión del sector. Esta afirmación se consolida en el documento al recogerse:

> *"Given such diversity, a one-cloud-fits-all solution will not serve all needs. Instead, the GC will adopt a Right Cloud strategy that will enable CIOs to have a number of cloud- and non-cloud deployment models to choose from".*

La libertad de decisión de la migración a la nube es, por tanto, la principal novedad que presenta el programa de Canadá. A diferencia de su homólogo en Reino Unido, que priorizaba el uso de la nube salvo que, por las circunstancias, principalmente los datos a tratar, no existiera causa justificada para ello, la *Right Cloud Strategy* de Canadá traslada la decisión, sin cortapisas, a los responsables de sistemas de las distintas administraciones u organismos.

Respecto a la operatividad de la contratación, presenta también una serie de particularidades. Al ceder el control directo de aspectos relacionados con la seguridad y la privacidad, siendo responsables las administraciones e instituciones de la confidencialidad, integridad y disponibilidad del servicio en la nube, el Gobierno de Canadá pretende facilitar la gestión del riesgo recomendando perfiles para evaluar la

---

[238] Se puede obtener más información en la web del departamento *Public Works and Government Services Canada*. Accesible en (apartado del evento): https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-033-28081. Último acceso: 08.08.2018.

[239] Publicada el 26.07.2016, actualizada el 25.06.2018. Accesible en: http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/it-ti/cloud-nuage/cas-san-eng.asp. Último acceso: 08.08.2018.

sensibilidad de los programas y servicios, definiendo los perfiles de control. Si bien, el Gobierno autorizará el uso del servicio y realizará un seguimiento continuo de la seguridad[240]. Aún no se ha liberado, se ha hecho público, cómo se estructurará la relación entre contratantes, proveedores y sistemas de control[241]. Sí se reseña que la práctica totalidad de los datos, para favorecer la seguridad de los datos y reforzar los perfiles, deberán ser almacenados en Canadá, salvo aquellos que la disponibilidad e integridad se consideren de perfil bajo. Algunos grandes proveedores, como Amazon, ya están aumentando sus *data centers* en la zona, adelantándose incluso a la versión definitiva del programa[242].

Otra de las variantes que plantea la *Right Cloud strategy* se encuentra en el mercado digital para la adquisición de los servicios de la nube, denominado *Canadian Public Sector Community Cloud* (CPSCC). Aunque son poco los datos que se conocen de este *marketplace*, el Gobierno ha mostrado que se va a circunscribir solo a un modelo de la nube: pública. Auspiciado por el *Public Service Chief Information Officer Council*, con el apoyo de las restantes administraciones o departamentos públicos, se pondrán a disposición de todas las organizaciones del sector público los servicios de las nubes públicas de aquellos proveedores que han acreditado la seguridad en sus servicios, conforme a las directrices marcadas por el Gobierno. Con los beneficios que tienen todos mercados digitales internacionales propuestos por los gobiernos para el uso de la nube, como la economía de escalas, apropiación de la experiencia de otros niveles de gobierno, control del servicio por un organismo autónomo y reducción de los esfuerzos en la

[240] Un desarrollo completo de los perfiles de control para la seguridad en el servicio se encuentra en la *Government of Canada Security Control Profile for Cloud-based GC IT Services*. Accesible en: http://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/itpm-itgp/it-ti/cloud-nuage/scp-pcs-eng.asp. Último acceso: 08.08.2018.

[241] Hasta la fecha, el Gobierno de Canadá solo ha publicado 3 documentos relacionados con la contratación en la nube:

- *Government of Canada Cloud Adoption Strategy*.
- *Government of Canada Right Cloud Selection Guidance.*
- *Government of Canada Security Control Profile for Cloud-based GC IT Services.*

[242] SILICON: "Amazon abrirá un primer centro de datos de almacenamiento en la nube en Canadá", 2016 (14.01.2016). Accesible en: http://www.silicon.es/amazon-abrira-un-primer-centro-de-datos-de-almacenamiento-en-la-nube-en-canada-2299783. Último acceso: 08.08.2018. Y QUINTANA, Eduardo: "Amazon alojará en Canadá un data center para la nube", *MCPRO*, muycomputerpro.com, 2016 (15.01.2016). Accesible en: http://www.muycomputerpro.com/2016/01/15/amazon-alojara-en-canada-un-data-center-para-la-nube. Último acceso: 08.08.2018.

búsqueda de una oferta adecuada; el listado de potenciales compradores se extiende, especial diferencia presentada respecto al programa de EE.UU., al Gobierno federal, gobiernos provinciales y territoriales, municipios, universidades, escuelas y hospitales.

d. Grupo de Trabajo IV (Comercio Electrónico) de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

En el seno de la CNUDMI, el Grupo de Trabajo IV ha intentado diseccionar los principales aspectos contractuales de la computación en la nube en diferentes periodos de sesiones con el fin de elaborar un documento que sirva de guía jurídica, marco contractual adecuado y previsible en el desarrollo del servicio informático, con el objetivo de ser particularmente útil para las pequeñas y medianas empresas. En el Capítulo II[243] hacíamos referencia al debate en torno al *cloud computing* que se estaba forjando en la CNUDMI, si bien no es hasta el 54º período de sesiones[244] cuando se ratifica la necesidad de realizar un documento descriptivo que recoja los aspectos contractuales más relevantes de este desarrollo informático, debiendo reflejar las prácticas contractuales más comunes y las normas técnicas pertinentes, cuando existieran.

Fruto de este mandato, la Secretaría informa al Grupo de Trabajo, y posteriormente a la Comisión, de los resultados de la labor preparatoria realizada en el ámbito de la computación en la nube[245]. La primera crítica es de índole política, al no considerarse oportuno un texto legislativo para la regulación del *cloud*, como una ley modelo o una guía legislativa. Esto limitará el alcance y el poder homogeneizador del texto en los ordenamientos nacionales. A la decisión estratégica anterior, el Grupo de Trabajo restringe aún más su estudio a la sola relación contractual entre empresas, es decir, en operaciones B2B. A nuestro entender, el ámbito de aplicación del texto, aunque recordemos que no tendrá carácter de texto legislativo, no cumple con la exigencia

[243] Capítulo II.d. "Principios comunes y específicos en el marco del comercio electrónico". En concreto, se estudiaba la propuesta del Gobierno de Canadá, en 48º período de sesiones (2015), sobre las "Cuestiones contractuales relacionadas con el suministro de servicios de computación en la nube".

[244] CNUDMI: "Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 54º período de sesiones" (Viena, 31 de octubre a 4 de noviembre), 2016. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/097/13/PDF/V1609713.pdf. Último acceso: 08.08.2018.

[245] Nota de la Secretaría - CNUDMI "A/CN.9/WG.IV/WP.142 - Aspectos contractuales de la computación en la nube", 2017, 55º período de sesiones. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V17/006/45/PDF/V1700645.pdf. Último acceso: 08.08.2018.

autoimpuesta por el Grupo de quiénes serán los beneficiarios potenciales del trabajo. En la nota de la Secretaría se señala que estos serán los que tienen *"menor poder de negociación"*. Cómo es posible, por tanto, que el texto no documente los problemas a los que se enfrentan los consumidores[246] cuando contratan el servicio de la nube. Aventuramos que la explicación no puede ser otra que la creación de un marco común de aspectos contractuales que no encuentre confrontación con las reglas tuitivas que rigen en defensa de los consumidores y usuarios o las normas que regulan las relaciones en el sector público. Sin embargo, conscientes de la cuota de mercado que puede representar los órganos administrativos en la contratación de la nube, advierten, aunque no entren en el estudio de las cláusulas, que las normas legales pueden imponer obligaciones a estos entes respecto a los sujetos contratantes, es decir, qué entidades pueden ser contratistas; qué datos pueden migrar a la nube; las condiciones y las normas que regularán la utilización del servicio, principalmente en materia de confidencialidad y privacidad; la posibilidad y la reglamentación en la subcontratación; las garantías necesarias que debe aportar el prestador del servicio; las obligaciones impuestas a los usuarios, especialmente al personal contratado por los organismos públicos; incluso la posibilidad de aumentar la responsabilidad de los proveedores, posición que no se corresponde cuando la parte contratante es un consumidor o una pequeña o media empresa.

Lo relevante en este período de sesiones es que se consolida el contenido y la estructura común de los contratos de computación en la nube, con base en la experiencia en el sector, que deberá replicarse en el futuro texto de desarrollo[247]. La libertad contractual y el régimen jurídico aplicable; la formación y forma del contrato, importante para identificar correctamente a las partes y los usuario del servicio; la descripción del servicio y los parámetros de calidad, determinando los servicios básicos y los opcionales o auxiliares, así como las normas técnicas y la supervisión y auditorías del servicio; la asignación de riesgos, ante los quebrantamientos de seguridad; el acceso a los datos por terceros; las cuestiones relativas sobre propiedad intelectual, principalmente sobre los derechos de acceso, las modificaciones de datos de los clientes, los datos procesados en

[246] El alcance de sus disposiciones para la protección de los consumidores se encuentra limitado por su propia configuración, razón de ser: *"principal órgano jurídico del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional"*. Sobre CNUDMI: http://www.uncitral.org/uncitral/es/about_us.html. Último acceso: 08.08.2018.

[247] Esta estructura coincide con las cláusulas de estudio del Capítulo V de nuestro trabajo, capítulo elaborado con anterioridad al debate de los aspectos contractuales de la nube en el Grupo de Trabajo IV de la CNUDMI.

la nube y los derechos derivados de la mejora por los usuarios; el precio y pago; la responsabilidad, con las posibles exenciones o limitaciones; la duración, prórroga y rescisión del contrato; las modificaciones de las condiciones del contrato, a lo largo de la ejecución; y la solución de controversias se configuran como las cláusulas mínimas de estudio para que de forma holística se pueda considerar debidamente tratado los aspectos contractuales de la computación en la nube.

El Grupo de Trabajo dio por concluido el examen de los aspectos contractuales de la computación en la nube, refrendando, salvo nimias cuestiones preliminares, el trabajo presentado por la Secretaría. Más prolijo resultó el debate sobre las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza[248]. Qué duda cabe que en un servicio informático global, donde los centros de datos se encuentran ubicados en diferentes localizaciones geográficas, la nacionalidad de los proveedores del servicio puede que no coincida con la nacionalidad de los sujetos contratantes y donde la normativa aplicable puede generar conflictos de competencia y aplicabilidad, un conjunto de instrumentos jurídicos que determinen las soluciones aplicables en la materia, que generen garantías y confianza en la identificación, fomentará la expansión del uso de la computación en la nube al aclarar y armonizar textos jurídicos, buscando la interoperabilidad jurídica como paso previo a la técnica.

A pesar de diferentes propuestas por los Estados para que el tratamiento y estudio de la materia se hiciera de forma autónoma y en una etapa ulterior[249], argumentario, entre otros, de la Federación de Rusia y de la delegación de los Estados Unidos, se establecieron una serie de temas que debía incluir esa labor de investigación y trabajo. Bajo el telón de fondo de los principios de autonomía de las partes, neutralidad tecnológica, equivalencia funcional y no discriminación, seis cuestiones debían considerarse: el reconocimiento jurídico, referido al *"uso de la gestión de la identidad con el fin de cumplir los requisitos legales exigidos para la identificación"*, no solo mediante disposiciones normativas o acuerdos, sino por el uso de determinadas credenciales; el reconocimiento mutuo, propugnando un marco de referencia común y considerando la experiencia de eIDAS

[248] CNUDMI: "Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 55º período de sesiones" (Nueva York, 24 a 28 de abril), 2017. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V17/029/31/PDF/V1702931.pdf. Último acceso: 08.08.2018.

[249] Como ocurrirá a partir del texto de análisis, es decir, en los períodos de sesiones siguientes la gestión de la identidad y los servicios de confianza se estudiarán de forma independiente y autónoma al estudio de la nube.

como sistema de gestión de la identidad; la atribución de información de identidad a un sujeto, que no necesariamente estaba relacionada con el nivel de garantía; la confianza y la atribución de acción, mensaje o firma a un sujeto; la asignación de los riesgos y la responsabilidad, debiendo determinar los operadores comerciales claramente ambas regulaciones; y la transparencia, en su doble vertiente de información de los métodos y procesos utilizados en la gestión de la identidad y los servicios de confianza, y en segundo lugar, con el deber de información ante quebrantamientos en la seguridad del servicio.

El marco propositivo del 55º período de sesiones se tradujo en el proyecto de lista de verificación sobre las principales cuestiones que podrían plantear los contratos de computación en la nube[250].

El estudio de los aspectos contractuales de la computación en la nube parte de la necesidad de realizar un análisis previo, por el contratante, ante la posibilidad de utilizar la herramienta informática. Esta es la razón principal por la que plantea, en primer lugar, una lista de verificación de aspectos precontractuales. El cliente debe prestar especial atención a la aplicabilidad imperativa de normas relacionadas con los datos personales[251], a la denominada ciberseguridad, a la incidencia que pudieran tener los derechos sobre propiedad intelectual en la fase contractual y post contractual y, en general, a cualquier normativa específica del sector a la que se pudiera estar sujeto. El documento elaborado concreta esta problemática en el estudio sobre la verificación de normas imperativas relacionadas con la ubicación de los datos, en materia de datos personales, de propiedad intelectual e industrial, de datos e información contables y de datos del sector público; y, en otra vertiente, en el análisis del contratista, no solo porque puede afectar a la ubicación de los datos, sino por las prohibiciones que podría imponer la normativa sectorial, piénsese en un proveedor extranjero que no cumpla las directrices del RGPD.

El *working paper* presentado en la nota de la Secretaría es un instrumento de gran labor pedagógica por la explicación de los riesgos potenciales a los que se enfrenta el cliente de la nube. Esta evaluación es primordial antes de trasladar nuestros datos,

[250] Nota de la Secretaría - CNUDMI "A/CN.9/WG.IV/WP.148 - Aspectos contractuales de la computación en la nube", 2018, 56º período de sesiones. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V18/003/92/PDF/V1800392.pdf. Último acceso: 08.08.2018.

[251] Será debidamente tratado en el Capítulo IV, principalmente en el apartado.b.

pudiendo ser obligatoria por imposición legal[252]. El proceder del cliente parte de la evaluación de la información sobre el proveedor de servicios en la nube elegido. El documento recoge que puede ayudar al cliente verificar las políticas de privacidad, confidencialidad y seguridad del proveedor, sobre todo por la prevención de accesos no autorizados y la política de datos en tránsitos; la garantía sobre metadatos, los registros de auditorías y registros de seguridad; la planificación o no de un plan de recuperación en casos de desastre; la asistencia en la migración, garantizando la interoperabilidad y transferibilidad; la capacitación de los empleados que intervienen en la cadena del servicio; las estadísticas de incidentes de seguridad; la certificación de una entidad independiente de las normas técnicas; la solvencia y la póliza de seguros; y el alcance en subcontratación. Esta evaluación previa tiene incidencia directa en la futura regulación contractual del servicio. Por consiguiente, un análisis profundo del proveedor en el desarrollo del servicio propiciará conocer el marco básico obligacional.

Aunque el documento no relacione estas medidas con la verificación de la ubicación de los datos, importante es conocer si el proveedor se encuentra obligado a realizar auditorías del servicio e, incluso, si el cliente tiene la posibilidad de realizar visitas sobre el terreno a los centros de datos. En cuanto a los riesgos asociados a la violación de los derechos de propiedad intelectual, propone que los clientes contraten los servicios con proveedores que utilicen estándares de código abierto o que, al menos, aporten la confirmación del consentimiento de terceros en el uso. Debe ser consciente, además, de los riesgos sobre la continuidad de las operaciones, es decir, si es posible una resolución anticipada de las partes; y de los conflictos relacionados con la estrategia de salida, vinculada principalmente a los datos subidos en la nube y las licencias de propiedad intelectual que permiten su uso con otro proveedor o fuera de la nube.

El documento propone una serie de recomendaciones sobre los riesgos denominados como dependencia tecnológica. Suelen ser riesgos no considerados por los clientes, sobre todo por aquellos que están menos familiarizados con las herramientas informáticas, pero pueden suponer el mantenimiento de una vinculación gravosa con un prestador de servicios. Por ello, remienda que el cliente se asegure la interoperabilidad y transferibilidad de los datos exportados a la nube, eligiendo proveedores que empleen

[252] Aunque no lo exponga el documento, sirva de ejemplo que, en determinados supuestos, el artículo 35 del RGPD establece la obligatoriedad de realizar una evaluación de impacto relativa a la protección de datos a los responsables del tratamiento.

procedimientos de exportación de datos no exclusivos y utilicen formatos de datos estándares o abiertos.

Esta exposición del análisis previo y de los riesgos potenciales en la contratación y utilización del servicio que se realiza para el Grupo de Trabajo IV de la Comisión, claramente mezcla aspectos que pueden ser evaluados de forma previa con un proceso de análisis que, de forma no dubitativa, solo podrá realizarse cuando esté en fase de formación del contrato. Seríamos ilusos, y el propio Grupo de Trabajo reconoce el desequilibrio de las partes en el poder negociador, si creemos que los proveedores del servicio nos facilitarán en una fase precontractual la política en materia de propiedad intelectual, confidencialidad, planes de recuperación, la ubicación exacta de los centros de datos o las estrategias de salidas, por citar solo algunos ejemplos. Tanto es así, que, incluso en el propio contrato, aspectos tan básicos como la ubicación de los centros de datos se determinan de manera difusa, amparando la redacción ambigua en la prevención ante posibles ataques informáticos. Esta labor de concienciación y de examen previo ante el cambio al servicio de la nube o ante un cambio de proveedor, que ha sido alabada *ad supra*, puede dificultar el alcance real de este análisis precontractual por no ser conscientes de la complejidad ni de las particularidades del sector. Determinar la responsabilidad de las partes en la migración, la clasificación de los datos que van a migrar a la nube, el nivel de protección adecuado o el calendario de la migración, por ejemplo, se regulará en un estadio más avanzado de análisis y contratación de la computación en la nube. Por lo tanto, aunque la elaboración de unas recomendaciones básicas para la correcta selección y contratación con un prestador de servicios supone un avance plausible que redundará en mayor transparencia y confianza en los clientes, el Grupo de Trabajo debería discernir entre las tareas propias a realizar en una fase precontractual y la incidencia de las cláusulas en la redacción del contrato, necesario, por la monopolización de grandes empresas tecnológicas que prestan el servicio.

Centrándonos en la lista de verificación de los aspectos relativos a la redacción del contrato, la primera crítica que debe realizarse del documento es la forma en la que se ha tratado la principal arteria en la contratación del *cloud*. Lejos de servir de manual de recomendaciones para la contratación de la herramienta informática, se configura como un dispositivo de advertencias. Siguiendo la estructura básica de los contratos de la nube, como marcaban los periodos de sesiones anteriores, bien podría haberse dispuesto a modo

de *check-list*. Esta disposición es fruto de la negativa de crear un instrumento normativo que regule la contratación del *cloud*, provista en el 55º período de sesiones.

No es el objetivo de nuestro estudio reproducir los dictámenes presentados al Grupo de Trabajo, pero sí es necesario reseñar los considerandos más relevantes, sobre todo por su aportación en la configuración del contrato de la nube como instrumento básico de reglamentación entre partes[253], teniendo siempre presente, como hemos indicado, que simplemente recoge las prácticas comunes que pueden afectar a la correcta ejecución de la relación contractual, no contribuyendo a ser un manual o instrumento de acciones a seguir que prevengan posibles riesgos futuros.

Las principales aportaciones se recogen dentro de las deferencias a las cláusulas que regulan la *"definición del objeto y ámbito de aplicación del contrato"*. Alertando al contratante sobre la relevancia de las disposiciones de los ANS, advierte que, ante contrataciones de servicios estandarizados, podemos encontrarnos con contratos que no recojan obligaciones específicas de resultados, incluso con redacciones laxas que no exijan un cumplimiento concreto, sino meras declaraciones de intenciones. El cliente debe optar, en la medida de sus posibilidades que estarán condicionadas a su poder de negociación, por ofertas que establezcan unos ANS con parámetros de desempeños cuantitativos y cualitativos, que permitan una evaluación concreta, con garantías de calidad y metodología para evaluar el cometido. Para la evaluación del desempeño, esta nota sí la establece el trabajo, es recomendable determinar períodos de referencia, frecuencia y forma de mecanismos de información y obligaciones de las partes. Respecto a las políticas de seguridad, señala que el cliente puede verse compelido a controlar sus propias medidas de seguridad, como la actualización de las claves de acceso de los usuarios de los servicios, pudiendo estar obligado a comunicar al proveedor los cambios en los mecanismos de gestión de identidad y acceso.

En materia de integridad de datos, insta a los clientes valorar si los proveedores asumen compromisos en la realización de copias de seguridad y si el acceso a dichas copias estaría fuera del alcance o influencia de los proveedores. Vinculada se encuentra la política en materia de protección de datos, privacidad y acuerdos de procesamiento, indicando que algunas jurisdicciones obligan a que el contrato contenga, como mínimo,

[253] Sí emplazamos al lector, para una adecuada valoración de nuestras aportaciones, al estudio del documento "A/CN.9/WG.IV/WP.148 - Aspectos contractuales de la computación en la nube", principalmente las páginas 12 a 38.

el objeto, duración, naturaleza y finalidad del procesamiento, los datos personales a tratar, así como el responsable y procesador de los datos. Como veremos en el Capítulo IV, la normativa aplicable en España establece un elenco de cláusulas, de contenido mínimo, que debe recoger el marco regulador ante el tratamiento de datos. Sobre la confidencialidad, propone al cliente la valoración de necesidades adicionales de protección, en función del contenido en la nube, formulando compromisos individuales de confidencialidad o restringiendo el acceso a determinados usuarios.

Respecto a las cláusulas relacionadas con los *"derechos sobre los datos del cliente y otros contenidos"*, nos recuerda el documento que los proveedores pueden tener derecho sobre los datos de los clientes, principalmente para tareas de supervisión de acuerdos y políticas de actuaciones. Considera necesario una revisión de las facultades otorgadas al proveedor, prestando especial atención a las posibilidades de transferencia a terceros y al ámbito geográfico y temporal de las potestades. En este marco se encuentran las actuaciones del proveedor ante un requerimiento del Estado solicitando datos e información del cliente, debiendo dedicar atención al análisis de la discrecionalidad del prestador del servicio en este supuesto, seleccionando aquel proveedor que, al menos, informe de inmediato del requerimiento de la autoridad. Si esta notificación incluye la categoría de los datos solicitados, el contratante tendrá un conocimiento más exacto de la amplitud y profundidad de las actuaciones, especialmente relevante cuando él es el responsable del tratamiento.

Idóneo es revisar, según el documento, las posibilidades de eliminación de datos, con especial ahínco en la fase de terminación y extinción del contrato. Es oportuno que revise si el prestador del servicio está obligado a eliminar los datos, los metadatos y las copias de seguridad, así como las normas o técnicas de eliminación empleadas, las autorizaciones requeridas para proceder a la eliminación y el calendario establecido para la realización de la actividad. Señala como medida especialmente garantista, la comunicación al cliente de la eliminación efectiva.

El contrato debe establecer las actividades de supervisión periódicas o recurrentes, determinando las responsabilidades y obligaciones de cada una de las partes, dentro de las cláusulas denominadas*"auditorías y supervisión"*. Auditorías que pueden incluir pruebas de seguridad, pudiendo las partes pactar que sea una entidad independiente quien las realice.

Los *"cambios en el servicio"* son comunes en los contratos de naturaleza informática, principalmente para adaptarse a las mejoras tecnológicas. Por este motivo, recomienda el texto analizar las cláusulas de actualizaciones, pudiendo obligar al proveedor a notificar al cliente con antelación sobre dichos cambios y sus consecuencias, aconsejando que se mantenga una versión en paralelo durante un plazo conveniente y considerando la asistencia del proveedor como una opción altamente recomendable. En este sentido, los proveedores suelen imponer cláusulas que eximen de la notificación ante los cambios de las condiciones del servicio, conminando al cliente a revisar con regularidad un apartado de la web del prestador. No puede obviarse, que lo más preocupante es que el proveedor suspenda el servicio por acontecimientos imprevisibles.

En las cláusulas referentes a los *"subcontratistas, proveedores del proveedor y externalización"*, los redactores se centran en informar al cliente que, ante proveedores que se reservan la capacidad de recurrir a terceros en la prestación del servicio, verifiquen que garantizan las medidas de seguridad, confidencialidad y protección de datos de la que goza el contratista en la subcontratación. Debe considerarse, al menos, según el documento, la notificación al cliente ante los cambios en la cadena de subcontratación, siendo recomendable reservarse el derecho de aprobación del cambio y la facultad de resolución del contrato ante los cambios propuestos.

Aborda la *"responsabilidad"* argumentando que los proveedores son propensos a excluir toda responsabilidad contractual, los prestadores de servicios consideran estas cláusulas innegociables. Añade, además, que cuando el prestador está dispuesto a asumir su responsabilidad, esta se encuentra limitada a aquellas infracciones que directamente están bajo su control, limitando la cuantía de pérdidas y los daños indirectos o derivados que puedan producirse. Las cláusulas sobre la responsabilidad del proveedor deben estudiarse con detenimiento en los contratos de adhesión, algunas medidas son claramente abusivas.

Los redactores del proyecto de aspectos contractuales de la nube son conscientes del servicio informático sobre el que se actúa, de ahí que centren parte del estudio a uno de los problemas que puede generar grandes conflictos por la evolución de la relación contractual y por la propia evolución de la herramienta informática, la *"duración y extinción del contrato"*. La fecha efectiva de la entrada en vigor de contrato sería conveniente dejarla meridianamente clara, porque el cliente puede requerir nuevas configuraciones o migrar los archivos a la nube. Uno de los problemas más característicos

es la dependencia tecnológica a un servicio, también abordado en la fase precontractual pero desde diferente óptica. Los proveedores suelen establecer períodos cortos de duración determinada del contrato y prórrogas automáticas del servicio. Por consiguiente, es oportuno discernir si el cliente tiene el derecho a ser informado de los plazos próximos de finalización del contrato y si existe la facultad de decidir, de forma efectiva, sobre la renovación del servicio. En este sentido, recuerda que las nubes estandarizadas suelen reservar al proveedor la posibilidad de resolver el contrato en cualquier momento, si bien algunos prestadores notifican al cliente la voluntad de rescindir el contrato. El sistema de notificaciones debe ser considerado en los supuestos de incumplimiento de las partes, con el objetivo de proceder a la subsanación de dicho incumplimiento, si este fuera posible, y en los supuestos de cambio de control por parte del proveedor, para lo que sería interesante que el cliente se reservase la posibilidad de resolver el contrato (por ejemplo, un cambio de titularidad en la compañía que presta el servicio).

Las *"obligaciones relativas a la finalización del servicio"* determinarán si el cliente tiene libertad real en la elección de proveedores de servicio en la nube. Dicta el documento que es recomendable seleccionar aquellos proveedores que en las cláusulas contractuales incorporen un plazo determinado para la exportación de datos e información, más si el cliente tiene acceso al contenido que se va a exportar, incluso si puede seleccionar las características, como el formato y procesos de exportación; asistan en el proceso de exportación, incluyendo el plazo y el alcance de la intervención; y recojan cláusulas de confidencialidad finalizada la relación contratada. Importante es atender a qué sucederá con los datos, es decir, cómo se eliminarán los datos de la nube en el proveedor primitivo. Por ello, el documento reconoce que el contrato debería incluir las normas de eliminación de los datos e información cuando ha sido debidamente exportado a otro proveedor o cuando ha concluido un plazo previamente establecido, incluso, la obligación de notificar al cliente antes de la eliminación definitiva de datos y metadatos.

Para finalizar, queremos destacar dos bloques de cláusulas contractuales que suelen ser habituales en los contratos de *cloud*, recogidas en el trabajo para el Comisión.

El cliente debe estudiar los mecanismos de solución de controversias; si se opta por el proceso arbitral, es oportuno examinar las normas que regirán el proceso; si se ha convenido sometimiento a un tribunal determinado; y si se determinan los plazos de prescripción para la presentación de reclamación. En este último supuesto, hay que tener

en cuenta si respetan los plazos mínimos obligatorios establecidos en la normativa de aplicación.

Las *"cláusulas de elección de la ley y el foro"* están íntimamente relacionadas con las anteriores. Teniendo presente que el derecho imperativo prevalece sobre las cláusulas de elección de la ley y el foro pactadas, exhorta al cliente a que preste especial cautela y estudio. Si las partes eligen el foro, debe chequearse los efectos de la ley elegida o aplicable y en qué medida se reconocerá y aplicará una resolución judicial de ese foro en los países donde se solicite su ejecución.

Como indicáramos al inicio de este opúsculo sobre el documento de aspectos contractuales relacionados con la computación en la nube, más que un instrumento propositivo, intentando solucionar o proponer recomendaciones ante conflictos o dificultades que puedan surgir en la fase precontractual, de ejecución o una vez terminado o resuelto el contrato, recoge una lista de cláusulas que pueden aparecer en el contrato habitual de la nube, advirtiendo al cliente de cómo el proveedor puede imponer medidas que perjudican, o pueden perjudicar, al contratante. En nuestro estudio se presentarán recomendaciones para que el cliente, independientemente de su poder negociador, pueda optar por un servicio en la nube que se adapte a sus necesidades, o al menos, que tenga la facultad de elegir, debidamente informado, el servicio más acorde. Emplazamos, por tanto, al análisis del Capítulo V, que siguiendo la estructura usual de los contratos de *cloud*, reconocida en los distintos documentos del Grupo de Trabajo IV, y en función de la naturaleza del sujeto contratante, analizará las cláusulas frecuentes en este tipo de contratos informáticos y las medidas a implantar, o que permitirán seleccionar a un proveedor sobre otro, para que el cliente equilibre su posición jurídica.

Por último, baste con reseñar que, en el 56º período de sesiones, los Estados Unidos de América[254] han propuesto, aunque directamente manifiesten que *"no ven la necesidad de que se elabore una lista de verificación sobre las principales cuestiones que podrían plantear los contratos de computación en la nube"*, que los documentos que desarrolle la CNUDMI en la materia no deban proporcionar asesoramiento jurídico ni dar la impresión de que favorecen a una de las partes del contrato. No es necesario argumentar, por todo

[254] Nota de la Secretaría - CNUDMI "A/CN.9/WG.IV/WP.151 - Aspectos contractuales de la computación en la nube - Propuesta de los Estados Unidos de América", 2018, 56º período de sesiones. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V18/003/92/PDF/V1800392.pdf. Último acceso: 08.08.2018.

lo expuesto en este subapartado, que claramente es la posición que ha adoptado la Comisión.

e. Conclusiones

De todos los programas y estrategias propuestos para la adopción en la nube podemos extraer que, al imponerse una serie de requisitos técnicos y unos programas de auditorías de seguridad de los servicios, las Instituciones pueden mitigar dos de los grandes riesgos que supone la asunción de esta tecnología, la dependencia a un proveedor de servicios y la continua mejora en seguridad. Propiciando la competencia entre proveedores con el mercado digital, siguiendo una estrategia de diversificación en la contratación y utilizando estándares abiertos, entre otros, garantizaremos que los costes de *lock-in* y *lock-out* se reduzcan considerablemente. Es más, la estrategia de la nube en Canadá se basa en los perfiles de programas de gestión de riesgos del programa FedRAMP (EE.UU.), con el objetivo de maximizar la interoperabilidad y la reutilización de pruebas. Empero sería imprudente considerar que estos costes se erradican con estas medidas, más cuando el modelo de implantación de la nube requiere un alto grado de diferenciación, como puede suceder con los servicios *SaaS*.

Por otra parte, todos los programas estudiados siguen, en mayor o menor medida, las evaluaciones del NIST. La evolución continua de la tecnología, estudiada a través del Instituto citado, se incorpora en los programas de implantación de la nube de referencia. Por lo tanto, aunque siempre se irá detrás de la evolución tecnológica, esta medida otorga ciertas dosis de dinamismo a la regulación del servicio.

Aún queda un largo camino por andar. En este estado embrionario solo se ha incorporado a clientes del sector público, consumidores que en gran medida tienen un gran poder negociador, ya sea de forma individual o asociada. Qué duda cabe que las novedades presentadas para los clientes gubernamentales se trasladarán a las entidades privadas, siempre y cuando los costes y estrategias del proveedor lo permitan. Sirva de ejemplo que cada vez son más los proveedores de la nube que instauran sus *data centers* en países con una normativa completa de protección de datos. En otro orden, y a pesar de los Acuerdos marcos, la regulación se centra en la seguridad del servicio en sus numerosas facetas. La labor de la CNUDMI pretende consolidar un marco propositivo para proteger a los sujetos con menor poder de negociación, en el marco de las relaciones privadas. Por lo tanto, el acervo de la Comisión tiende a estructurar la relación contractual

B2B, siempre bajo el prisma de los principios reconocidos para el comercio electrónico. Sin embargo, precisamente el carácter no holístico ni imperativo pueden mermar su influencia en los ordenamientos jurídicos nacionales.

Estas fallas en el mercado de la computación en la nube habilitan y refuerzan el interés público por regular de una manera global el *cloud*. Además, conforme se discutió en el Capítulo II, las propias estructuras y el contexto en el que se desenvuelve la computación en la nube potencian una regulación propia. Sin embargo, una de las características comunes a los servicios que nacen al albur de la red es la imposición de las reglas de Internet, fuera de la capacidad de ordenación de los ordenamientos jurídicos estatales, junto con la propia independencia al funcionamiento. No podemos obviar que la red y las actividades y servicios que se desarrollan a su amparo pecan de un déficit democrático en la regulación de las relaciones jurídicas entre partes, un fenómeno global que puede dejar al margen la participación de actores con escaso poder de influencia en la elaboración de su normativa. Esta circunstancia habilita a considerar que la contratación de la nube deba regirse, al menos respecto a los derechos y obligaciones más primarios, por regulación expresa, dictada por Instituciones nacionales, supranacionales o transnacionales que garanticen un mínimo común denominador, no solo respecto a los pequeños o medianos usuarios y contratantes del servicios de la nube, sino en relación a los pequeños y medianos proveedores del servicio que quedan excluidos en un sector altamente sectorizado, donde los grandes prestadores de servicios informáticos, en general, ocupan altas cuotas de mercado.

La adhesión a contratos tipos por los usuarios de los servicios, impuestos no solo por los prestadores de servicios sino por los suministradores de intermediación, han conformado unas condiciones generales homogéneas. Una regulación, no solo limitada a actores relacionados con la Administración pública, que garantice la seguridad de las comunicaciones y que propicie un equilibrio en la contratación entre partes, dejando al margen la mayoría de las relaciones jurídicos-privadas, puede ser el punto de partida para crear un marco de un unión entre el contenido contractual desarrollado hasta la fecha y una tutela respecto a ámbitos típicos del Derecho público, como pueden ser los ilícitos relacionados con la propiedad intelectual, añadiendo una defensa a ciertos colectivos, como los consumidores en sentido estricto. En esta correlación de intereses, por tanto, no debe desconectarse los aspectos con contenido jurídico-públicos con las relaciones jurídico-privadas, si bien, debe facilitarse el juego de la autonomía de la voluntad en el

ámbito privado siempre garantizando la correcta igualdad de partes. Por consiguiente, la manera de garantizar la asunción de los principios comunes del comercio electrónico, tratados en el Capítulo II, desarrollados en gran medida en el Anteproyecto de Código Mercantil, estudiados en el aparatado a. del presente Capítulo, debe ser la configuración de un régimen jurídico que proporcione reglas susceptibles de ser aplicadas.

Los actores privados tienen diferentes propósitos en el régimen de regulación de la computación, y estos diferentes objetivos incorporan dimensiones que interfieren en el interés público. En los programas implantados en el ámbito internacional, analizados *ad supra*, ha sido la seguridad en la protección de los datos, en toda su extensión, el centro de atención de los gobernantes. Cómo compatibilizar una normativa sobre la contratación en la nube con el carácter internacional de la prestación del servicio es una cuestión fundamental. Una buena alternativa puede ser acudir al *soft law* internacional, como tantas otras veces ha sucedido en materia de comercio electrónico. Frente a los límites que pueden presentar los ordenamientos jurídicos nacionales con una regulación *ex novo* de la contratación de la nube, una regulación conjunta que incorpore estándares internacionales diseñados por la industria combinado con las premisas necesarias para garantizar la adecuación con el interés público y la autonomía de la voluntad de los actores, puede propiciar la correcta evolución, uniformidad y legitimidad, que no obligatoriedad, que requiere la regulación de un servicio acostumbrado a regirse por las reglas que se autoimpone la red.

CAPÍTULO IV – DISPOSICIONES REGULATORIAS, SU INCIDENCIA EN EL CONTENIDO DEL CONTRATO. **a. El contrato para garantizar la seguridad, la protección y el equilibrio en el *cloud computing*. b. Cliente y proveedor en el contrato de la nube a la luz de la normativa protectora de datos de carácter personal**: *a. Acceso a los datos por el prestador de servicios en la nube. b. Subcontratación en la prestación de servicios de cloud computing. c. Transferencia internacional de datos personales. d. Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.*

CAPÍTULO IV – DISPOSICIONES REGULATORIAS, SU INCIDENCIA EN EL CONTENIDO DEL CONTRATO

a. El contrato para garantizar la seguridad, la protección y el equilibrio en el *cloud computing*

Los diferentes marcos jurídicos nacionales y la incertidumbre sobre la normativa aplicable, incluso dentro del mercado único, propiciado por los contenidos digitales y la deslocalización de los mismos, favorece la aprobación de acuerdos contractuales que respeten el paradigma del servicio en la nube, y con ello un mercado único digital. La complejidad en la gestión del servicio y sus patrones de uso, unido a la necesidad de generar y mantener la confianza y la seguridad de la información y datos que se exportan a los servidores de los prestadores del *cloud computing*, reclaman un marco jurídico previsor para los clientes del servicio.

Los contratos actuales que regulan el servicio recogen cláusulas que inciden, principalmente, en el acceso a los datos y su portabilidad, el control de las modificaciones de la información y la propiedad de los datos trasladados al *cloud*. Al tratarse mayoritariamente de cláusulas predispuestas por el proveedor de la nube, la seguridad del acceso y el mantenimiento de datos no encuentran un desarrollo detallado, principal preocupación, la seguridad, confidencialidad y privacidad en sentido amplio, cuando contratan Instituciones del sector público. Unas cláusulas contractuales equilibradas garantizarían una seguridad jurídica que la proliferación de normas no puede aportar, estandarizando un nivel adecuado de interoperabilidad en los datos, salvaguardando la portabilidad, y estableciendo medidas para la protección de los datos personales.

Desde un marco regulatorio, previsiblemente a través de la herramienta contractual, el sector público, así como los agentes privados, pueden beneficiarse de unos servicios económicamente ventajosos, salvaguardando la compatibilidad del servicio con la

normativa estatal y comunitaria, no solo en términos normativos sino económicos[255], proveyendo un marco competitivo, abierto y seguro.[256]

De los estudios de la Comisión Europea[257] se destaca que una mayor transparencia en el tratamiento de los datos contribuirá a generar confianza en los consumidores, por lo que aspectos como la protección de los datos[258], la legislación aplicable o la dificultad de determinar la reglamentación de las transferencias internacionales de datos decaerían como principales problemas en la adopción de la computación en la nube[259]. Resalta la Comisión, que el Derecho contractual es motivo de especial preocupación por afectar negativamente a la confianza digital de los consumidores, al no tener seguridad sobre sus derechos y el sistema de protección de los mismos, y de los comerciantes, que necesitan un marco que les facilite sus productos en línea.

En este proceder, esta Institución establece como acción clave 2, para la potenciación de la computación en nube en Europa, unas condiciones contractuales seguras y justas.

---

[255] Tan importante es la incidencia económica en los contratos que el Premio Nobel de Economía de 2016 se otorgó a Oliver Hart y Bengt Holmström por su "Teoría de los Contratos". Se puede obtener más información en la web oficial de los Premios Nobel. Accesible en: http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/. Último acceso: 08.08.2018.

[256] En 2016 Microsoft, Amazon e IBM ya superaban los 10.000 millones de dólares de ingresos, de forma independiente, gracias a la nube. PRIETO, Miriam: "Amazon, Microsoft, Google e IBM libran la gran batalla del 'cloud computing'", *Expasión.com*, 2016, noticia de 01.11.2016. Accesible en: http://www.expansion.com/economia-digital/companias/2016/11/01/581381d8e5fdea8e3e8b4587.html. Último acceso: 08.08.2018.

[257] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Liberar el potencial de la computación en nube en Europa, 2012, COM (2012) 529 final (27.09.2012). Accesible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2012:0529:FIN. Último acceso: 08.08.2018.

[258] Se ha tratado en el Capítulo III.b. como el Grupo de Trabajo del artículo 29 se ha centrado en la protección de los datos personales en la utilización de los servicios de la nube. Este Grupo envió una misiva al consejero delegado de Whatsapp, tras adoptar la tecnología del *cloud* y pasar a formar parte del grupo empresarial Facebook, por el intercambio de datos entre ambas entidades y las dudas sobre su legalidad. No es pública la contestación de la compañía. MORENO, Víctor: "La UE solicita que Whatsapp interrumpa el intercambio de datos con Facebook", *Expasión.com*, 2016, noticia de 28.10.2016. Accesible en: http://www.expansion.com/economia-digital/companias/2016/10/28/58133c5bca4741c87f8b45a2.html. Último acceso: 08.08.2018.

[259] Recientemente, la justicia francesa ha condenado a Twitter por incluir cláusulas abusivas que perseguían utilizar los datos personales con fines publicitarios de forma ilícita. ELDIARIO.ES: "La justicia francesa condena a Twitter por incluir cláusulas abusivas para hacer negocio con los datos personales", *eldiario.es,* 2018, noticia de 10.08.2018. Accesible en: https://www.eldiario.es/tecnologia/justicia-francesa-Twitter-clausulas-personales_0_801770541.html. Último acceso: 10.08.2018.

Alerta de una débil seguridad en los contratos con los proveedores de servicios en nube, siendo el desequilibrio y la regulación parcial de los paradigmas que plantea el servicio las causas principales. La complejidad de la nube y la incertidumbre jurídica en el uso del *cloud computing* hace que se recurra, de manera excesiva, a Acuerdos de Nivel de Servicios, donde las características esenciales son la complejidad y la exoneración de responsabilidad por parte de los prestadores. Hay que añadir que el uso excesivo de cláusulas contractuales tipo limitan la capacidad de negociación de los usuarios, debiendo asumir, por ejemplo, la legislación aplicable o la imposibilidad de recuperación de sus datos.

MARZO PORTERA[260] argumenta que las empresas y el sector público se han subido al barco de este "progreso tecnológico" y se arriesgan a contratar servicios de *cloud computing* sin las garantías legales oportunas, obviando incluso diferentes procedimientos administrativos y empresariales. Contratando los servicios vía web, estos actores están adhiriéndose a unas condiciones generales que impone el proveedor, sin posibilidad alguna de negociación por parte de los agentes. Se agrava, más si cabe, cuando se conviene con prestadores de servicios ubicados en terceros países (concepto empleado por las Instituciones europeas para referirse a Estados fuera del Espacio Económico Europeo), donde es común cláusulas de exoneración de responsabilidad, incluso en aspectos tan importantes como el acceso a los datos, no cumpliendo con la normativa europea al respecto. La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[261] y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público[262] obligan a las Administraciones públicas a adaptarse a las nuevas tecnologías existentes, compeliendo a estos entes a prestar servicios a través de medios electrónicos, que requieren compartir información y

[260] MARZO PORTERA, Ana María: "Privacidad y cloud computing, hacia dónde camina Europa". *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, 2012, nº 8, p. 225.

[261] Accesible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10565. Último acceso: 08.08.2018.

[262] Accesible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10566. Último acceso: 08.08.2018.

sincronización entre Instituciones, para que los interesados puedan cubrir el elenco de procedimientos que abarcan[263].

Se debe prestar especial atención, en consonancia con las directrices del Comité Económico y Social Europeo[264], a las "condiciones generales". Esta Institución informa que la gratuidad del servicio puede resultar muy gravosa en pérdidas de tiempo e información. No se puede olvidar que los servicios gratuitos pueden implicar costes no financieros[265]. Del mismo, al ser un contrato en el que raramente las condiciones son negociables, posteriormente ahondaremos en el clausulado de manera detallada, se debe de prestar especial atención a los siguientes puntos:

- El nivel de servicios de computación en la nube.
- La disponibilidad de los datos y la responsabilidad en el supuesto de pérdida, daño o indisponibilidad de los mismos.
- La exclusividad o no de los recursos empleados.
- Determinación de los criterios de consumo, y las posibilidades y criterios para la escalabilidad de los servicios.
- Los condicionantes necesarios para la transmisión de información y datos a un tercero ajeno a la relación contractual.
- La identidad exacta de las partes contratantes y los prestadores de servicios.
- Los supuestos de rescisión del contrato, por ambas partes.
- La jurisdicción y la reglamentación que se le aplican al contrato.

Como mecanismo para la protección de los clientes, se propone establecer una política corporativa con las condiciones a aplicar a los contratos de *cloud*, con el fin de contrastar cada oferta de los proveedores de la nube con un marco de referencia, incluyendo los objetivos estratégicos de la entidad, el procedimiento de aprobación de las iniciativas del

[263] En el Capítulo V.c. se abordará de manera detallada la contratación de la nube por los entes del sector público.

[264] Dictamen del Comité Económico y Social Europeo sobre el tema "La computación en nube (*cloud computing*) en Europa" (Dictamen de iniciativa), 2012 (26.10.2011). Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52011IE1606&from=ES. Último acceso: 08.08.2018.

[265] Sirva como ejemplo los proveedores 4shared (http://www.4shared.com/) o Uploaded (http://uploaded.net/), que además de limitar la velocidad de comunicación, establecen publicidad en sus servicios *cloud* gratuitos. Por otra parte, indicar, que estos servidores *free* suelen tener un "ciclo de vida" corto, desapareciendo rápidamente y dejando de estar operativos, con las implicaciones que tiene en los datos trasladados a la nube.

cloud, requisitos técnicos (seguridad, privacidad, portabilidad e interoperabilidad), tratamiento específico que requieran las aplicaciones, infraestructuras o datos y requisitos mínimos para su contratación. Un mecanismo parecido a los Acuerdos marcos del G-Cloud de Reino Unido con un abanico mayor de requisitos esenciales. De esta forma, se plantean como necesarias la inclusión de cláusulas en el contrato que determinen el alcance del servicio, niveles de servicios y disponibilidad que el proveedor debe satisfacer, las localizaciones físicas donde residirán nuestros datos, las obligaciones que asume el proveedor de servicios respecto a la seguridad y la protección de los datos, la responsabilidad del proveedor, la extinción y la rescisión anticipada del contrato, la posibilidad de la migración de los datos y la titularidad de los datos y aplicaciones[266]. Sin embargo, la negociación de las cláusulas contractuales se encontrará como límite las exigencias que imponga la normativa regulatoria y las propias exigencias corporativas del prestador de servicios y la empresa cliente.

Es oportuno recordar las aportaciones de la Data Protection Act 1998 de Reino Unido, que pone de manifiesto el ICO[267], para el tratamiento de datos. Establece como exigencia la constatación por escrito de un contrato con el procesador de datos. Con ello, el proveedor del *cloud* se compromete a no cambiar las condiciones que regulan las operaciones en el procesamiento de datos durante la vida del contrato sin el conocimiento y consentimiento del cliente de la nube. De esta forma, el encargado del tratamiento de datos actuará siguiendo las instrucciones del responsable del tratamiento de los datos, cumpliendo las obligaciones de seguridad equivalentes a la que le corresponderían a aquel. Esto no exime a los clientes que contraten estos servicios de prestar especial atención a los términos y condiciones que establecen los proveedores, más cuando supone un "lo tomas o lo dejas", ya que determinarán si tienen suficiente control sobre sus datos.

En los informes de la ENISA se destaca cómo en las etapas iniciales de implantación del *cloud computing*, ante una deficiente y parca regulación jurídica, los aspectos

[266] MORALES, José Ramón: "Cloud computing: Riesgos corporativos e implicaciones jurídicas", *Actualidad jurídica Aranzadi*, 2013, nº 863, p. 11-14.

[267] INFORMATION COMMISSIONER'S OFFICE (ICO): "Guidance on the use of cloud computing: Data protection act 1998", 2012, v. 1.1.

contractuales devienen en una importancia capital para la seguridad y la protección de las operaciones y los datos aportados[268].

Para finalizar, una nota debemos traer a colación al estudiar la seguridad y privacidad en el entorno de la nube. Recientemente, el Senado de EE.UU. ha aprobado la *Clarifying Lawful Overseas Use of Data Act*[269], conocida como *CLOUD Act*, una norma que permite acceder a los datos que un proveedor de servicios nacional almacena fuera de las fronteras del país. Un prestador de servicios de la nube se puede ver compelido a revelar los datos e información perteneciente a un cliente, con independencia de dónde se encuentren localizados los centros de datos. La norma, laxa en los requisitos necesarios para el efectivo requerimiento de acceso a los datos y difusa en los ítems que llevarían al tribunal a modificar o anular el contenido del requerimiento promovido por la autoridad policial[270], nace a raíz del Caso Warrant[271], que pretendía la aplicación extraterritorial de las normas de EE.UU., en concreto, acceder a datos e información de un cliente alojados en servidores de Microsoft en Irlanda. Con la promulgación de la *CLOUD Act*, los ciudadanos, como clientes, pueden ver mermadas la privacidad, transparencia y seguridad de datos y comunicaciones, entre otros derechos, cuando el proveedor de servicios tenga domicilio social en EE.UU.

---

[268] ENISA: "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

[269] Accesible en: https://www.congress.gov/bill/115th-congress/house-bill/4943. Último acceso: 08.08.2018.

[270] *"Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—"(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government; "(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and "(iii) the customer or subscriber is not a United States person and does not reside in the United States."*

[271] U.S. Supreme Court Microsoft Corp. v. United States, 17.04.2018, 584 U.S. Accesible en: https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf. Último acceso: 08.08.2018.

b. Cliente y proveedor en el contrato de la nube a luz de la normativa protectora de datos de carácter personal

El estudio debe comenzar con la delimitación conceptual de encargado de tratamiento de los datos personales para que, posteriormente, puedan conocerse las implicaciones jurídicas del proveedor de los servicios de *cloud computing* al amparo de la normativa protectora sobre datos personales. Destacaba la Comisión Europea[272] que *"la protección de datos se considera uno de los más graves obstáculos para la aceptación de la computación en la nube"*, instando al Consejo y al Parlamento a adoptar una propuesta de Reglamento tan pronto como sea posible. Fruto de esta necesidad, el 4 de mayo de 2016 se publica en el Diario Oficial de la Unión Europea el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, RGPD, que será de aplicación[273] frente a Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, normativa nacional sobre protección de datos personales que cumple con las pautas de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[274]. En el Considerando 7 del RGPD se recoge *"estos avances* (la rápida evolución tecnológica y la globalización) *requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales"*.[275]

---

[272] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Liberar el potencial de la computación en nube en Europa, 2012, COM (2012) 529 final (27.09.2012). Accesible en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2012:0529:FIN. Último acceso: 08.08.2018.

[273] Aplicable desde el 25 de mayo de 2018, artículo 99.

[274] La LOPD continúa vigente formalmente, siendo aplicables los preceptos que no entren en contradicción con RGPD, de aplicación directa en todos los Estados miembros. A la fecha, como posteriormente se indicará, está en tramitación parlamentaria el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, que vendrá a completar la regulación contenida en el RGPD.

[275] Como recuerda MARTOS, el RGPD establece la protección de datos personales como un derecho no absoluto, debe relacionarse con su función en la sociedad, manteniendo el equilibrio con otros derechos fundamentales. MARTOS, Natalia: "Se acerca el 25 de mayo de 2018. ¿Está su empresa adaptada al nuevo

En el *cloud computing*, la delimitación entre responsables y encargados del tratamiento de datos se encuentra difuminada *"por la pluralidad de sujetos intervinientes en el tratamiento de los datos vinculado a las distintas esferas que en dichos servicios se traduce la capacidad de decisión sobre la finalidad, contenido y uso de los datos personales que permiten identificar al responsable de los mismos"*[276]. La implantación de la tecnología 2.0, así como la contratación y utilización de la computación en la nube dificultan la clara distinción clásica entre el responsable y encargado del tratamiento, incluso entre la correcta delimitación de los titulares de los datos personales[277].

El Grupo de Trabajo del artículo 29[278] resalta que *"la aplicación concreta de los conceptos responsable del tratamiento de datos y encargado del tratamiento de datos se está haciendo cada vez más compleja. Esto se debe ante todo a la creciente complejidad del entorno en el que se usan estos conceptos y, en particular, a una tendencia en aumento, tanto en el sector privado como en el público, hacia una diferenciación organizativa, combinada con el desarrollo de las TIC y la globalización, lo cual puede dar lugar a que se planteen cuestiones nuevas y difíciles y a que, en ocasiones, se vea disminuido el nivel de protección de los interesados"*. Por lo tanto, las definiciones

Reglamento de Protección de Datos?*, Diario La Ley*, 2017, núm. 9081, sección Tribuna. Acceso a través del servicio digital La Ley Digital (bajo suscripción).

[276] RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012, p. 88.

[277] FERNÁNDEZ ALLER, Celia: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)", *Revista de Derecho UNED*, 2012, núm. 10, p. 131. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/11093/10621. Último acceso: 08.08.2018. PEDRAZA CÓRDOBA reitera que la evolución del *cloud* dificulta la separación entre el responsable y el encargado del tratamiento, especialmente relevante para determinar la responsabilidad de las partes. PEDRAZA CÓRDOBA, Juanita: "Los riesgos sobre la privacidad de los datos personales en un entorno cloud computing: una aproximación desde el reglamento europeo de protección de datos", *Revista de Privacidad y Derecho Digital,* 2017, núm. 6, p. 98-105.

[278] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"", adoptado el 16.02.2010, 2010, 00264/10/ES WP169, p. 2.

contenidas en el artículo 2, letra d) y e) de la Directiva 95/46/CE deben ser tratadas con cautela[279]. Definiciones que se mantienen en el RGPD[280].

De este modo, la posición jurídica del proveedor de servicios de *cloud computing* dependerá de las propias características del servicio prestado y la posibilidad de decidir sobre la finalidad, el contenido y el uso del tratamiento de los datos. GARCÍA DEL POYO[281] amplía el espectro de posibilidades que puede suponer el desarrollo del servicio de la computación en la nube a un supuesto de comunicación de datos a terceros, conforme a lo recogido en el artículo 11.2.c LOPD.

Sin embargo, en términos generales, podemos establecer que los prestadores de los servicios en la nube, aun pudiendo tener una importante capacidad para la toma de decisiones de los datos que le son confiados determinando las medidas de seguridad oportunas o la propia subcontratación de los servicios, tienen limitadas sus facultades, serán los clientes quienes sigan ostentando la capacidad para determinar la finalidad, contenido y uso del tratamiento, por lo que conservarán la condición de responsables del tratamiento. Esta posición jurídica del cliente se refuerza, como indica RUBÍ NAVARRETE[282], por la capacidad de decisión sobre la contratación del servicio, la selección de la compañía prestadora del servicio y las garantías que deben llevarse a cabo. En el mismo sentido se manifiesta GARCÍA MEXÍA[283]. GARCÍA argumenta que la puesta a disposición de los datos por parte del cliente de la nube al proveedor de servicios no implica la cesión o comunicación en sentido estricto, al recaer entre el proveedor y el

[279] En la citada Directiva, se consideraba responsable del tratamiento a *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario"*; y como encargado del tratamientos a *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento"*. En nuestro ámbito normativo, ambas definiciones se recogen en el artículo 3, letra d) y g) de la LOPD, respectivamente.

[280] Véase el artículo 4, apartados 7) y 8).

[281] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 69.

[282] RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012, p. 94.

[283] GARCÍA MEXÍA, Pablo: "Cloud computing: Sus implicaciones legales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2010, nº 23, p. 84.

cliente un contrato de servicio. Por consiguiente, no sería necesario el consentimiento del titular de los datos. De esta forma, quien contrata los servicios de la nube no pierde la condición de responsable del fichero o tratamiento, y el proveedor de servicios cumple la función de mero encargado del tratamiento, debiendo seguir las instrucciones que el responsable del fichero le imparta. No se tiene presente en el debate, sin embargo, cómo limitan el poder decisorio de los clientes las cláusulas predispuestas por los proveedores, sobre todo las grandes compañías.

Ser responsable del tratamiento de los datos personales implica determinar para qué y por qué se va a producir el tratamiento de datos, no solo desde una posición formal, que implicaría siempre que el cliente de la nube sea el responsable, sino de forma material o de hecho. Por lo tanto, quien determina las operaciones de tratamiento cuando un cliente se acoge a cláusulas predispuestas por grandes empresas del sector. El RGPD establece como obligación informar a los interesados de las condiciones en las que se realiza el tratamiento de datos, debiendo materializarse por escrito, de forma concisa, transparente, inteligible, de fácil acceso y con un lenguaje claro y sencillo. Esta información deberá contener, como novedades, la base jurídica del tratamiento, la intención o no de realizar transferencias internacionales de datos, los datos del delegado de protección de datos si lo hubiere y si se elaboran perfiles de interesados.

El estatuto real del cliente deberá depender de la influencia del mismo para determinar el control del tratamiento de datos. Se ha hecho hincapié en que el cliente decide la finalidad, uso y tratamiento de los datos, y, cuando el proveedor de la nube añada o modifique estos aspectos, deberá ser considerado responsable del tratamiento. Las concentraciones del servicio en grandes compañías limitan la completa libertad de aceptación de las cláusulas contractuales, que suelen presentarse como un "lo tomas o lo dejas". Los desequilibrios en el poder negociador de las partes no deben presuponer que el cliente se encuentre esclavo de las condiciones contractuales del gran operador, si bien, la evolución del *hardware* y *software*, para una completa funcionalidad, pueden exigir la contratación del *cloud* a unos prestadores determinados. El Grupo de Trabajo del artículo 29[284] advertía de los riesgos que podría suponer la contratación de la nube derivados de la falta de control de los datos o de la deficiente información sobre el tratamiento. Sirva

[284] GRUPO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: "Dictamen 5/2012 sobre la computación en la nube", adoptado el 01.07.2012, 2012, 01037/12/ES WP196, p. 6 y 7.

de ejemplo las Condiciones Generales para Ofertas de Cloud de IBM[285]. Tras recoger expresamente que *"el Cliente es el único responsable de cualquier dato personal incluido en el contenido, y designa a IBM como encargado para tratar dichos datos personales"*, señala que *"IBM, sus filiales y sus terceros proveedores podrán tratar, almacenar y usar los datos de la cuenta en cualquier lugar en el hagan negocio para habilitar características de los productos, administrar su uso, personalizar la experiencia y, de cualquier otra manera, dar soporte al uso del Servicio de Cloud y mejorarlo. Por datos de la cuenta se entenderá toda la información (que puede incluir datos personales) acerca del Cliente o de sus usuarios proporcionada a, o recogida por, IBM"*.

La AEPD[286] atajó la discusión considerando que el prestador de servicios en nube debe ser considerado encargado de tratamiento, siendo el cliente responsable, en todo caso, del tratamiento al decidir la finalidad, contenido y uso de tratamiento. De igual forma ha sido tratado por el Grupo de Trabajo del artículo 29 en su Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012[287], aclarando que, si los prestadores de los servicios en la nube no atienden a las propias instrucciones del cliente, sino que actúan con plena autonomía, deben ser considerados responsables del tratamiento. El RGPD instaura la figura de delegado de protección de datos y el nuevo contenido mínimo del contrato de encargo en el tratamiento, reforzando el poder, real, decisorio del cliente del *cloud*. En su artículo 28, hace recaer en el cliente de la nube la correcta selección de un encargado de tratamiento de datos, proveedor de la nube, demostrando que este aplica correctamente las prescripciones establecidas en la norma[288].

---

[285] Vigentes a 08.08.2018. Accesible en: http://www-03.ibm.com/software/sla/sladb.nsf/pdf/5948-02/$file/i126-5948-02_01-2017_es_ES.pdf. Último acceso: 08.08.2018.

[286] AEPD: "Orientaciones para prestadores de servicios de Cloud Computing", 2013, p. 5. La guía ha sido actualizada en el año 2018. A los efectos estudiados, continúa con las mismas consideraciones. AEPD: "Orientaciones para prestadores de servicios de Cloud Computing", 2018, p. 5-6. Accesible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf. Último acceso: 08.08.2018.

[287] Véase Capítulo III.b: Actividad del Grupo Europeo de Protección de Datos "artículo 29".

[288] Artículo 28.1 del Reglamento UE 2016/679 del Parlamento Europeo y del Consejo: "*Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado*".

La delimitación conceptual y jurídica proyecta en los clientes de los servicios de *cloud computing*, responsables de los ficheros, un deber de actuar con suma cautela en la elección del prestador de los servicios en la nube, asegurándose que se cumplen unas medidas protectoras y de seguridad de protección de datos idénticas a las que exige la Unión Europea, en el supuesto de que dicho proveedor no se circunscriba al ámbito de aplicación de la normativa comunitaria. Un nuevo aporte del Reglamento permite la aplicación de la normativa europea en el marco de las actividades desarrolladas en el establecimiento del responsable o del encargado del tratamiento, independientemente de dónde se realiza el tratamiento de datos. Como señala DÍAZ DÍAZ[289], *"en un entorno globalizado como el tecnológico, la aplicación extraterritorial de las normas constituye un verdadero desafío, pues no tendría demasiado sentido limitarlas a un determinado espacio, ..., o a un concreto conjunto de personas".* El artículo 3.2 del RGPD reconoce dentro de su ámbito territorial de aplicación a los tratamientos realizados por responsables o encargados no establecidos en la Unión siempre que sus actividades de tratamientos estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, con independencia de si se requiere pago por el servicio; o cuando el control de su comportamiento tenga lugar en gran medida en la Unión Europea. Habría que añadir el criterio contenido en el artículo 3.1 del RGPD, considerando aplicable el Reglamento, aun cuando el tratamiento no se realice en el territorio de la Unión, si es dentro de un contexto de actividades de un establecimiento del responsable o de un encargado en la Unión. En palabras de PEDRAZA CÓRDOBA[290], *"esta separación entre las acciones del tratamiento y las ejecutadas propiamente en el territorio de la Unión, consulta adecuadamente el carácter descentralizado del modelo cloud"*. Esta ampliación del ámbito de aplicación territorial supone un aval y una cobertura, al garantizar el derecho de protección de datos a los ciudadanos europeos ante los grandes proveedores de la nube, que suelen residir fuera del territorio de la Unión Europea[291].

[289] DÍAZ DÍAZ, Efrén: "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones". *Revista Aranzadi Doctrinal*, 2016, núm. 6/2016, p. 169-170.

[290] PEDRAZA CÓRDOBA, Juanita: "Los riesgos sobre la privacidad de los datos personales en un entorno cloud computing: una aproximación desde el reglamento europeo de protección de datos", *Revista de Privacidad y Derecho Digital,* 2017, núm. 6, p. 108.

[291] El desarrollo de los representantes de responsables o encargados del tratamiento no establecidos en la Unión se regula en el artículo 27.

Cuando analicemos los contratos de la computación en la nube, podrá vislumbrarse que la portabilidad de los datos que se encuentran en el entorno informático es requisito esencial para que, de manera real y efectiva, el cliente tenga libertad de elección del proveedor. El RGPD recoge en el artículo 20 el derecho del interesado a solicitar al responsable del tratamiento, cuando se realice de forma automatizada, su recuperación en un formato que permita el traslado a otra entidad responsable, incluso de manera directa entre responsables de datos. Por lo tanto, el cliente de la nube deberá garantizar la portabilidad no solo por criterios de buena gestión del negocio, sino para el cumplimiento de los deberes que le marca el Reglamento para con los interesados.

Partiendo de la delimitación de los sujetos intervinientes en el *cloud computing*, es necesario ahondar en el contrato de la nube a la luz de la normativa sobre protección de datos.

a. Acceso a los datos por el prestador de servicios en la nube.

Con la contratación del *cloud computing*, el prestador de servicios en la nube intervendrá, realizará tratamientos, en la información y datos que el cliente haya traspasado o cree en el servicio informático. La relación entre cliente y proveedor se desarrollará a través del contrato de acceso a datos. El responsable del fichero traslada a los distintos prestadores que intervienen en la cadena de suministro las condiciones y garantías a adoptar, con el fin de asegurar el nivel mínimo de protección que exige el RGPD, antes la Directiva 95/46/CE, por lo que cada parte solo tiene plena libertad en las cuestiones relacionadas con la llevanza de su negocio siempre que no contradigan las cláusulas contractuales reguladoras de las condiciones y las garantías en materias de protección de datos[292]. Sin embargo, el cliente es responsable de la correcta elección del proveedor, artículo 28.1 del RGPD, porque como indica el artículo 20.2 del RLOPD, *"cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el*

[292] MARZO PORTERA, Ana María: "Privacidad y cloud computing, hacia dónde camina Europa". *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, 2012, nº 8, p. 215.

cumplimiento de lo dispuesto en este Reglamento"[293]. La regulación del contrato de acceso ya se establecía en el artículo 12 LOPD, configurando el acceso a los datos por cuentas de terceros[294].

La celebración de un contrato, *"por escrito o en alguna otra forma que permita acreditar su celebración y contenido"*, que recoja las instrucciones que el responsable del tratamiento impone al prestador de servicios, limitando su actividad a las indicaciones dadas, era la primera exigencia de la LOPD. De este modo, el prestador de servicios debía detallar de manera exhaustiva qué servicios presta y el responsable del tratamiento los servicios requeridos. Esta relación, que fomenta el intercambio de información entre las partes, parece determinar que el poder de decisión sobre el tratamiento de los datos sigue residiendo en el cliente de la nube. *"El contrato es la expresión de la relación jurídica entre el cliente -responsable- y el proveedor de servicios de la nube -encargado-, y su existencia y unos contenidos mínimos se derivan del artículo 12 LOPD"*[295], lo que exige un deber de colaboración, transparencia y diligencia entre las partes, condicionantes no siempre presente cuando el prestador es una gran entidad que remite, para su contratación, a unas condiciones generales de contratación y a los ANS. El RGPD, manteniendo igualmente la necesidad de celebrar *"un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros",* presenta como novedad la ampliación, de manera expresa, del contenido mínimo del contrato de encargo de tratamiento, debiendo contener, entre otros aspectos, el objeto, la duración, la naturaleza y la finalidad

---

[293] Como hemos indicado anteriormente, el artículo 28.1 Reglamento UE 2016/679 del Parlamento Europeo y del Consejo recoge idéntica obligación del responsable del tratamiento, siguiendo la línea emprendida por el Grupo de Trabajo del artículo 29 y la AEPD.

[294] Artículos 12.2 y 12.4 de la LOPD: "*2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.*
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
...
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.".

[295] COTINO HUESO, Lorenzo: "Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"". *Revista catalana de dret públic*, 2015, nº 51, p. 97.

del tratamiento, el tipo de datos personales y categorías de interesados, las obligaciones y derechos del responsable, la previsión de confidencialidad de las personas que tratarán los datos, la asistencia del encargado para la correcta aplicación por el responsable de los derechos ejercitados por los interesados, la supresión o devolución de los datos al finalizar el encargo, la obligación de poner en disposición del cliente toda la información que demuestre la correcta aplicación de la normativa, y permitir y contribuir a la realización de auditorías e inspecciones por el cliente o por un auditor autorizado por el responsable[296].

Este es el contenido mínimo, también, para las subcontrataciones en el tratamiento de datos personales, sin perjuicio de que las cláusulas contractuales tipo que regula el Reglamento sirvan como base. Las partes en todo caso deberán respetar los límites que se establecen en el propio Reglamento. Deberán atender, al menos, a las medidas de seguridad que establece el artículo 32; se impondrá al encargado la necesidad de requerir consentimiento previo antes de proceder a la subcontratación, exigiéndole además que la relación se materialice en un contrato por escrito con las mismas garantías que las iniciales; y deberá recogerse el compromiso de respetar la confidencialidad en el tratamiento, tratando los datos personales únicamente sobre las instrucciones documentadas del responsable. Aunque determina que el encargado *"pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable"*, no aparece en el texto normativo su desarrollo, debiendo materializarse en el contrato. Sería oportuno y conveniente, pues, que las autoridades nacionales dotaran de un contenido de mínimos a una obligación de tanta importancia en materia de seguridad y confianza.

Por exigencia expresa del artículo 28.2 del RGPD, único requerimiento que se recoge de forma taxativa en el artículo 12 LOPD, de otra forma carecería de sustantividad el acceso a datos, el contrato celebrado con el prestador de servicios debe establecer la finalidad para la cual se formula. Este fin determinará el uso de los datos encargados al proveedor del *cloud*, no pudiendo utilizar los datos con una finalidad distinta a la establecida. Impondrá, del mismo modo, la obligación al encargado del tratamiento de no

[296] Artículo 28.3 del RGPD.

comunicar los datos a otras personas, ni siquiera para su conservación (*"ni los comunicará, ni siquiera para su conservación, a otras personas"*, redacción del artículo 12 de la LOPD).

De una lectura rápida pudiera parecer que no cabe la participación de terceros en la prestación del servicio. RUBÍ NAVARRETE[297] estimaba que no debía hacerse una interpretación restrictiva del precepto, es el propio RLOPD quien admite, en el artículo 21, la posibilidad de que el encargado del tratamiento subcontrate actividades relacionadas con la prestación del servicio siempre que se establezcan las garantías apropiadas. El RGPD resuelve las dificultades en la interpretación del precepto al establecer una regulación más prolija del tratamiento de datos por terceros. Al ser objeto de análisis en el subapartado posterior, emplazamos su estudio al examen de la subcontratación del servicio del *cloud*.

En otro orden de cosas, el contrato con el proveedor de servicios en la nube debe contener las medidas de seguridad previstas en la ejecución de la prestación de servicios[298]. Este requisito aparece establecido en el 12 de la LOPD, guardando relación

---

[297] RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012, p. 98.

[298] Sirva como ejemplo las medidas de seguridad establecidas en Dropbox, protección no solo para los archivos o datos almacenados sino para las transferencias entre el *software* gestor y los propios servidores (archivos en tránsito). Si bien, no cumple en profundidad con las exigencias de la LOPD, ni por ende del RGPD, dado que no discrimina en función de los datos que estemos almacenando y, en algunas conexiones no declaradas a los usuarios, los datos en tránsito no están protegidos:

"Los archivos de Dropbox y los documentos de Dropbox Paper almacenados se cifran mediante el estándar Advanced Encryption Standard (AES) de 256 bits. Para proteger los datos en tránsito entre las aplicaciones de Dropbox (actualmente para escritorio, móviles, API o web) y nuestros servidores, Dropbox emplea las tecnologías Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para la transferencia de datos, creando un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior. De manera similar, los datos en tránsito entre un cliente de Paper (para dispositivos móviles, API o web) y los servicios alojados siempre están cifrados mediante SSL/TLS"

Versión 08.08.2018. Accesible en: https://www.dropbox.com/business/trust/security/architecture. Último acceso: 08.08.2018.

Puede observarse como la política de seguridad de Dropbox tiende a dar menor información a los clientes, focalizando su política a la privacidad de los datos más que a los medios de seguridad, al menos en la información comunicada a los usuarios. Véase, como ejemplo, la política de seguridad que contenía su web en dos fechas anteriores:

Versión 20.12.2016:

"Para proteger los archivos en tránsito, Dropbox usa el protocolo SSL/TLS para la transferencia de archivos; de este modo, se crea un túnel seguro protegido por cifrado AES de 128 bits o más. Los datos de los archivos de Dropbox se guardan en bloques de archivos discretos que se fragmentan y cifran mediante

con el contenido del artículo 9 de dicho texto legal. De esta forma, las exigencias en el nivel de seguridad sobre el responsable del tratamiento de los datos personales, según la propia naturaleza de los datos objeto de tratamiento, se reflejarán en el encargo del tratamiento de datos. El RGPD refuerza la exigibilidad en materia de seguridad, ya que a las medidas de seguridad del tratamiento que conmina el artículo 28.3.c, en relación con el artículo 32, incorpora la asistencia al responsable de datos en medidas técnicas y organizativas del servicio, así como las propias del cliente del tratamiento; a lo que habría que añadir la ya comentada responsabilidad del cliente en la elección de un encargado del tratamiento que reúna las medidas técnicas y organizativas adecuadas.

El principal problema aparece cuando los encargados del tratamiento de datos son entidades de terceros países, dada la posible disparidad en la regulación de los tratamientos de datos personales. De esta forma, y como apunta RUBÍ NAVARRETE[299], los estándares ISO, o similares, se presentan como una vía adecuada para que los

---

AES de 256 bits. No todos los reproductores multimedia de dispositivos móviles son compatibles con la transmisión cifrada; por lo tanto, los archivos multimedia transmitidos desde nuestros servidores no siempre están cifrados. Además, respaldamos la confidencialidad de la comunicación, marcamos todas las cookies de autenticación como seguras y habilitamos la política HSTS".

Versión 20.12.2016 - Fuente: https://www.dropbox.com/security#protection. Último acceso: 20.12.2016. Actualmente el acceso redirecciona a la versión actual.

Versión 14.09.2013:

"Ciframos los archivos que almacenas en Dropbox mediante AES-256, que es el mismo estándar de cifrado que emplean los bancos para proteger los datos de sus clientes. El cifrado del almacenamiento se aplica después de subir los archivos, y nosotros gestionamos las claves de cifrado. Dropbox utiliza Amazon S3 como solución para el almacenamiento de datos. Amazon los almacena en varios centros de datos a gran escala. Amazon afirma que utiliza acotamiento de control de perímetro de grado militar, vigilancia de vídeo y personal de seguridad profesional para mantener sus centros de datos físicamente seguros. Encontrarás más información acerca de la seguridad de Amazon en el sitio oficial de los servicios web de Amazon. Amazon y Dropbox también emplean medidas significativas de protección contra riesgos de seguridad, como los ataques de denegación de servicio distribuida (DDoS), los ataques de intermediario (MITM o "Man in the Middle") y el rastreo de paquetes.
Tus archivos se envían entre los clientes de escritorio de Dropbox y nuestros servidores a través de un canal seguro que emplea un cifrado SSL (Secure Sockets Layer) de 256 bits, el estándar para las conexiones seguras a través de Internet. Tus archivos se envían entre las aplicaciones móviles de Dropbox y nuestros servidores a través de un canal seguro, con cifrado SSL de 256 bits siempre que es posible. No todos los reproductores de medios móviles son compatibles con la difusión cifrada, de modo que los archivos multimedia difundidos desde nuestros servidores no siempre están cifrados."

Versión 14.09.2013 – Fuente: https://www.dropbox.com/security. Actualmente el acceso redirecciona a la versión actual.

[299] RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012, p. 94.

prestadores de *cloud computing* cumplan con las medidas de seguridad establecidas[300]. En el Capítulo III, apartado experiencias internacionales, se ha observado cómo los organismos gubernamentales han optado por imponer estándares ISO, principalmente ISO/IEC 17020:2012[301], para determinar la adecuación de los proveedores de la nube con los que contratar. COTINO HUESO[302] considera que, para generar una relación de confianza y seguridad entre los sujetos intervinientes en el contrato de la nube, sobre todo por los riesgos que asume el cliente en la protección de datos personales y su responsabilidad, debe implantarse en el servicio la adopción de estándares técnicos. Estas consideraciones se han plasmado en la nueva norma europea. El artículo 42.1 del RGPD recoge "(los) *Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"*, indicando, expresamente en el artículo 43.1.b, la necesaria adecuación a la norma EN ISO/IEC 17065/2012, sin perjuicio de requisitos adicionales establecidos por la autoridad de control. Sin embargo, especialistas en el sector consideran al ISO/IEC 27018:2014 más adecuado al nuevo Reglamento europeo[303]. La aplicación práctica de la norma dictaminará el modelo de referencia.

La relación e intercambio de información entre encargado y responsable del tratamiento debe llevar a garantizar las medidas de seguridad que el RGPD pretende,

---

[300] Aunque posteriormente se tratará la transferencia de datos a terceros países, y siguiendo el estudio de Dropbox, la certificación *Privacy Shield* y *Shafe Harbor* refuerza la imagen al exterior de la aplicación de medidas de seguridad estándares en el almacenamiento y transición de datos. Accesible en: https://www.dropbox.com/help/security/data-transfers-europe-us. Último acceso: 08.08.2018.

[301] Revisión a fecha de 20.12.2016.

[302] COTINO HUESO, Lorenzo: "Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"". *Revista catalana de dret públic*, 2015, nº 51, p. 100.

[303] Además del propio Cotino Hueso; Ricard Martínez, Luis de Salvador y Nicolas Schifano consideran al ISO 27018 como el marco útil para proporcionar confianza en el cumplimiento de la normativa de protección de datos en la nube. VVAA: "Nuevo Estándar de Seguridad y Privacidad en Cloud Computing: ISO 27018", *FIDE (Fundación para la Investigación sobre el Derecho y la Empresa)*, 2014, conferencia 12.12.2014. Accesible en: http://www.fidefundacion.es/Resumenes-de-sesiones-y-foros_a170.html. Último acceso: 08.08.2018. Nota de prensa en ELDERECHO.com: http://tecnologia.elderecho.com/tecnologia/privacidad/fide-cloud_computing-iso_27018-estandar_de_seguridad_y_privacidad_0_772125190.html. Último acceso: 08.08.2018.

desde un punto de vista más material y funcional que formal. La Agencia Española de Protección de Datos[304] indica que los avances tecnológicos como la informática en la nube demuestran que, en la práctica, las multinacionales dedicadas a la prestación de servicios globales a terceros precisan de un instrumento análogo a las Normas Empresariales Vinculantes, recogidas actualmente en el artículo 47 del RGPD, aplicables a los encargados de tratamiento, para garantizar un nivel adecuado de protección en el tratamiento de los datos personales dentro de la estructura empresarial. Este instrumento y marco regulador permite la flexibilización en la autorización de transferencias internacionales de datos en el seno de las multinacionales. Igualmente, destaca la Agencia Española de Protección de Datos, que la creación de dicho instrumento debe tomar como referente los principios establecidos en la Decisión de la Comisión 2010/87/UE[305].

En este proceder, es necesario estudiar las previsiones que el RLOPD, que recordemos sigue estando vigente hasta una nueva norma y aplicable en lo no regulado por el RGPD, establece para los proveedores de *cloud computing*, entendiendo a estos como encargados de tratamientos de los datos personales[306].

Exige el artículo 88.5 del RLOPD que el documento de seguridad incorpore referencia expresa del contrato o documento que regula las condiciones del encargo, por lo cual reitera la relevancia de un contrato expreso que determine la ejecución del servicio y la

[304]AEPD: "Contribución de la Agencia Española de Protección de Datos a la consulta de la comisión sobre un enfoque global de la protección de datos personales en la Unión Europea", 2011. Accesible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/aepd_dpa_es.pdf. Último acceso: 24.12.2016.

[305] En el subapartado .c se desarrolla, de forma detallada, la aplicabilidad e incidencia de las Normas Empresariales Vinculantes y las cláusulas tipo de la Decisión 2010/87/UE.

[306] Artículo 88.5 del RLOPD: "*Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo".*

Artículo 88.6 del RLOPD: *"En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.*
En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento".

adopción de las medidas de protección que la normativa establece[307]; la identificación de los ficheros o tratamientos que se traten en concepto del encargo del servicio; la identificación del responsable; y el período de vigencia del encargo. Dicha observancia cumple con las premisas establecidas del actual artículo 28.3 del RGPD, anteriormente recogidas en el artículo 17.3 de la Directiva 95/46/CE, al obligar al responsable del fichero o tratamiento a suscribir un contrato con el encargado del tratamiento, para que el proveedor de servicios actúe siguiendo las instrucciones del responsable del fichero o tratamiento. El RGPD incorpora, además, la prohibición de recurrir a otro encargo sin la preceptiva autorización previa, por escrito, del responsable del tratamiento.

La siguiente exigencia, establecida en el artículo 88.6 del RLOPD, se pondrá de manifiesto dependiendo de los servicios que los proveedores de computación en la nube ofrezcan, dado que el ámbito de aplicación hace referencia a que los *"datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado"*, añadiendo que *"tal circunstancia afectase* (debe afectar) *a parte o a la totalidad de los ficheros o tratamientos del responsable"*. Por lo tanto, se hace necesario delimitar previamente los servicios contratados para determinar la aplicabilidad del precepto. Siendo aplicable dicho precepto, cuando se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable de los mismos debe anotarlo en el documento de seguridad correspondiente. En el segundo supuesto, cuando se realice el tratamiento total o parcialmente en los sistemas de prestador de servicios, el responsable puede delegar el documento de seguridad al encargado del tratamiento de los datos, salvo en aquellos datos mantenidos con recursos propios[308].

[307] En el Capítulo II hacíamos referencia al contenido natural del contrato del *cloud*. En resumen, y con independencia del modelo de implantación, complejidad y atipicidad del contrato de la nube, su contratación permite almacenar la información de manera permanente en distintos servidores a través de los cuales los usuarios pueden recuperar la información mediante Internet cuando así lo requieran los clientes, a través de unos procedimientos establecidos que requieren la externalización de los servicios. De igual modo, el contenido natural del contrato de acceso a datos, aunque no se defina de manera expresa en la LOPD, regula el acceso a los datos personales para la prestación de servicios por el encargado del tratamiento en ficheros cuya responsabilidad pende del responsable del tratamiento.

[308] El RGPD no establece como obligatorio la elaboración de un documento de seguridad, si bien, puede ser un instrumento propicio para garantizar las medidas de seguridad que establece la norma. Cabe recordar que el RGPD parte de una actuación proactiva del responsable y del encargado del tratamiento de datos, que exige estar en disposición de demostrar las actuaciones que realizarían los sujetos ante incidentes en materia de seguridad.

La figura creada con el RGPD, el delegado de protección de datos, dependiente del responsable, encargado o profesional independiente en el marco de un contrato de servicios, será el encargado de ofrecer asesoramiento acerca de la evaluación de impacto[309] para la protección de datos al responsable y encargado del tratamiento. Asesorará sobre las obligaciones de las partes (responsable y encargado), será la persona de contacto en lo referente al tratamiento de datos, principalmente ante una violación de la protección, y gestionará y supervisará el cumplimiento de la normativa, artículo 39. Debe ser el complemento perfecto al registro de tratamientos de datos, regulado en el artículo 30, que exige contabilizar y definir, entre otros aspectos, los tratamientos de datos en el seno de la entidad, los datos personales que se recogen o tratan y las medidas de seguridad adoptadas por las empresas para la realización del correcto tratamiento.

Como decimos, el delegado de protección de datos es la persona responsable de informar al responsable o al encargado del tratamiento de las obligaciones que les impone el RGPD, teniendo, además, una labor supervisora y en continua cooperación con la autoridad de control. Esta figura será obligatoria para las entidades públicas y para las personas jurídicas de carácter privado que realicen tratamientos de datos especiales por la naturaleza, alcance y fines, o por las categorías especiales de datos a tratar.

Es necesario reflexionar sobre la correlación entre el conocimiento, o autorización, del documento de seguridad del prestador de servicios con la práctica habitual de la contratación del *cloud computing*, donde los clientes, responsables del fichero o tratamiento, tienen poca determinación en la negociación de las medidas de seguridad del prestador, más si cabe cuando la contratación de los servicios se realiza con entidades multinacionales que tienen un amplio abanico de clientes.

Hemos mostrado las dificultades de la citada dicotomía responsabilidad-contratación externa con grandes compañías, concluyendo que deben flexibilizarse las exigencias de la normativa reguladora de protección de datos, salvo que por la cantidad de datos tratados o la especial protección a los mismos requieran un tratamiento más rígido. El RGPD no distingue entre niveles de seguridad en los ficheros, habla de medidas de seguridad

[309] Recomendamos, para un conocimiento de qué supone la evaluación de impacto en el RGPD, la lectura de PUYOL, Javier: "Especial consideración de la Evaluación de Impacto en el Reglamento General de Protección de Datos de la Unión Europea (RGPDEU) y en sus normas de desarrollo", *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's,* 2018, Tirant lo Blanch.

adecuadas al riesgo de los datos[310], lo que no significa que no tenga que realizarse una evaluación de los datos e información a tratar. Hay que atender, por tanto, a la naturaleza de los datos para adecuar el proceso de seguridad del *cloud computing*. RUBÍ NAVARRETE[311] plantea los criterios que deben servir de punto de referencia para la correcta adecuación de las medidas de seguridad en la prestación del servicio:

- Que sean jurídicamente vinculantes los documentos de seguridad prestados, lo que implica determinar la jurisdicción competente que exigirá el cumplimiento.
- Que una Autoridad de Protección de Datos pueda analizar la actividad del responsable del tratamiento, y así determinar su adecuación con la normativa y la relación contractual. El RGPD refuerza la actividad fiscalizadora de la AEPD, en España.
- Que los interesados tengan posibilidad de resarcirse económicamente cuando se vulnere el régimen de garantías protectoras, conforme a la ley nacional aplicable al responsable que contrata el servicio.

El RGPD incorpora, como novedad, una presunción de cumplimiento de las medidas de seguridad cuando el responsable o el encargado del tratamiento se adhiera a un código de conducta o mecanismo de certificación, artículo 32.3. Esta evaluación de seguridad, tomada de forma voluntaria, es un instrumento de transparencia y redundará en mayor confianza por y para los clientes.

Con estas premisas, las obligaciones establecidas en el artículo 28 del RGPD, y el desarrollo del artículo 88 del RLOPD, para el responsable y el encargado del tratamiento de datos, se encuentran salvaguardadas.

Se ha indicado anteriormente que el RGPD establece la necesidad de llevar un registro, de cada actividad, en el que los responsables y encargados detallen las

[310] Sin embargo, como señala RICARD MARTÍNEZ, debe hacerse una lectura integrada de la normativa. Es por ello que el artículo 81 del RLOPD, que normativiza los niveles de seguridad, sigue siendo adecuado y de aplicación como elemento normativo adicional. MARTÍNEZ, Ricard: "Las medidas de seguridad en el Reglamento general de protección de datos", *LOPD y Seguridad* (blog personal), 2016, entrada de 20.12.2016. Accesible en: http://lopdyseguridad.es/gdpr1/. Último acceso: 08.08.2018.

[311] RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012, p. 101.

actividades de tratamiento de datos, con la información contenida en el artículo 30[312]. La obligación de documentación será exigida para las entidades que cuenten con 250 o más trabajadores y aquellas entidades que lleven a cabo tratamientos de datos que puedan comportar un riesgo, no ocasional, para los derechos y libertades de las personas interesadas, incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

El reconocimiento y positivación del "derecho al olvido", también llamado "olvido digital" o "supresión", supone uno de los avances más esperados en la nueva norma europea. Aunque su aplicación al *cloud computing* no resulta tan evidente como en los buscadores web, la supresión de los datos personales de los afectados puede resultar de vital importancia ante proveedores de dudosa legalidad. Este requerimiento está encomendado al responsable del tratamiento, obligado, para lo que requerirá la indudable colaboración del proveedor de la nube. Cuando el ciudadano conocedor de que sus datos son tratados por el responsable de datos, o incluso por el proveedor del servicio de la nube, de manera que no se ajusta a la normativa aplicable, o que simplemente retira su consentimiento previo, decide ejercitar su derecho de supresión inmediata, el cliente de la nube (responsable del tratamiento) requerirá del encargado del tratamiento la efectiva actuación informática para su correcta ejecución. Por lo tanto, sería oportuno fijar entre las partes el procedimiento para la correcta aplicabilidad del "derecho al olvido". Entre otros, el plazo a transcurrir entre la comunicación del responsable al proveedor para su efectiva supresión o los criterios para la ponderación entre el alcance del "derecho al olvido" y los derechos de libertad de expresión, salud pública o deber de conservación. Pocas compañías ofrecen la posibilidad de ejercitar correctamente el derecho de referencia, más todo lo contrario, los prestadores del servicio recogen dentro de sus políticas de privacidad que la eliminación de los datos puede no realizarse de forma inmediata. Google[313], para sus servicios[314], establece:

---

[312] Para los responsables se encuentra regulado en el artículo 30.1, para los encargados del tratamiento el contenido se delimita en el artículo 30.2.

[313] PRIVACIDAD y CONDICIONES de GOOGLE, CÓMO CONSERVA GOOGLE LOS DATOS QUE RECOGE. Política vigente a 08.08.2018. Accesible en: https://policies.google.com/technologies/retention?hl=es. Último acceso: 08.08.2018.

[314] Incluye productos que desarrollan tecnología *cloud* como Chrome OS, Chrome (explorador) y Fiber.

"Como ocurre con cualquier eliminación de eliminación, pueden producirse retrasos en los procesos y los periodos establecidos en este artículo debido a actividades de mantenimiento rutinarias, interrupciones inesperadas del servicio, errores o fallos de nuestros protocolos"[315].

El desarrollo práctico de la prestación del servicio de *cloud computing* ha mostrado que parte de los servicios han sido subcontratados a entidades ajenas a la relación contractual principal. MARZO PORTERA[316] considera que la caracterización de este modelo de negocio se basa *"en la continua subcontratación de servicios y descentralización geográfica y transfronteriza de base de datos que pueden almacenar información sobre individuos o personas"*. Para atender a esta realidad y confrontarlo con la normativa española de protección de datos, en el próximo subapartado se estudiará la subcontratación de los servicios de la computación en la nube.

Por último, el RGPD regula, esencial para salvaguardar en última instancia los derechos de los interesados en el marco del *cloud computing*, la notificación que el encargado de tratamiento de datos debe realizar al responsable, *"sin dilación indebida"*, de las violaciones de seguridad en los datos personales de las que tenga conocimiento. Este deber de comunicación a los responsables de datos y a las autoridades de control se ve completado con la comunicación de la violación de seguridad de los datos personales al interesado. La comunicación a los responsables, aunque la obligación encuentre exenciones en el propio texto, debe hacerse en un lenguaje claro y sencillo, recogiendo, como mínimo, la naturaleza de la violación, los datos de contacto del delegado de protección de datos, las posibles consecuencias de la violación de seguridad y las medidas

[315] La nueva redacción de PRIVACIDAD y CONDICIONES DE GOOGLE ya supone un avance. La POLÍTICA DE PRIVACIDAD DE GOOGLE, revisión de 29.08.2016, vigente 23.02.2017, era aún más laxa. Establecía:

"Aunque elimines tus datos de nuestros servicios, es posible que no destruyamos de inmediato las copias residuales almacenadas en nuestros servidores activos ni los datos almacenados en nuestros sistemas de seguridad".

[316] MARZO PORTERA, Ana María: "Privacidad y cloud computing, hacia dónde camina Europa". *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, 2012, nº 8, p. 214.

adoptadas para corregirla o mititigarla. Coincidimos con MARTÍNEZ[317] en que la responsabilidad del cliente debe nacer del *accountability*, por lo que incluso la falta de notificación del encargado del tratamiento[318], imputable a este, al responsable del tratamiento conlleva un incumplimiento de las obligaciones del contratante de la nube[319], al establecerse en el propio Reglamento el principio de diligencia en la elección del encargado.

El principio de *accountability*, promulgado en el RGPD, obliga al responsable del tratamiento de datos a aplicar las medidas oportunas y eficaces, que *"ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas"*. Esta responsabilidad activa o proactiva conlleva la aplicación de instrumentos que den cumplimiento al mandato normativo, como la adhesión a códigos de conducta o la certificación; la protección de datos desde el diseño y por defecto, artículo 25; al establecimiento de medidas técnicas datos; al registro de actividades, artículo 30; y la evaluación de impacto, artículo 35, como contrapartida a la eliminación por el RGPD del deber de registro de los ficheros ante la autoridad de control[320]. Dentro de las medidas de seguridad específicas, según el riesgo de la organización, es imprescindible citar la seudonimización, el cifrado de los datos personales, la garantía de la confidencialidad, integridad, disponibilidad y resiliencia permanente en los servicios de tratamiento, y la posibilidad de restauración de la disponibilidad y el acceso rápido ante incidentes físicos o técnicos. Las nuevas previsiones establecidas por el RGPD son relevantes para el entorno de la nube porque,

---

[317] MARTÍNEZ, Ricard: "Las medidas de seguridad en el Reglamento general de protección de datos", *LOPD y Seguridad* (blog personal), 2016, entrada de 20.12.2016. Accesible en: http://lopdyseguridad.es/gdpr4/. Último acceso: 08.08.2018.

[318] El artículo 33.2 solo recoge que *"el encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento"*.

[319] El artículo 33.1 establece la obligación del responsable del tratamiento, en caso de violación de seguridad, de notificar *"a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación"*.

[320] MARTOS, Natalia: "Se acerca el 25 de mayo de 2018. ¿Está su empresa adaptada al nuevo Reglamento de Protección de Datos?, *Diario La Ley*, 2017, núm. 9081, sección Tribuna. Acceso a través del servicio digital La Ley Digital (bajo suscripción).

como indica ÁLVAREZ HERNANDO[321], se extienden al encargado del tratamiento cuando subcontraten servicios que impliquen acceso a datos, con otros subencargados.

b. Subcontratación en la prestación de servicios de cloud computing.

El Real Decreto 1720/2007, de 21 de diciembre, RLOPD, parte negando la posibilidad de la subcontratación a un tercero en el tratamiento de datos, salvo autorización del responsable del tratamiento, contratación que si se efectúa será en nombre y por cuenta del responsable del tratamiento de datos. No específica, sin embargo, si debe ser consentimiento expreso o no. Este límite material que impone el Real Decreto, al ser necesaria la autorización del responsable del tratamiento y perdiendo el encargado del tratamiento el poder de disposición de los datos encomendados, restringe un buen desarrollo práctico del servicio de computación en la nube.

La rigidez inicial es matizada por el artículo 21.2 del RLOPD, más propicio para el desarrollo técnico de la nube. Permite la subcontratación de los servicios sin necesidad de la autorización del responsable de los datos, siempre y cuando se cumplan una serie de requisitos. En primer lugar, requiere que la posibilidad de subcontratación de los servicios del *cloud computing* se recoja dentro del objeto del contrato entre el responsable y el encargado del tratamiento de datos, estableciéndose la empresa con la que se va a subcontratar el servicio. Cuando no fuere posible concretar la empresa subcontratista, el encargado del tratamiento debe comunicar al responsable los datos relativos de la entidad que va a hacer frente al servicio antes de que se proceda a la subcontratación.

Contrastando este primer requisito de la subcontratación sin necesidad de autorización del responsable con la práctica de los servicios en la nube, aunque posteriormente se desarrollarán las cláusulas contractuales establecidas en el *cloud*, suele ser común que en el contrato se recoja un listado amplio de entidades con las que se pueden subcontratar los servicios. Es más, la experiencia en el servicio de la nube demuestra que esta lista sufre variaciones a lo largo de la duración del contrato entre el prestador de servicios de *cloud* y el responsable de los datos. Sin embargo, no todos los marcos contractuales detallan las posibles empresas que pueden ser subcontratadas. Por ello, parece oportuno que para cumplir las directrices que establece la normativa se

[321] ÁLVAREZ HERNANDO, Javier: "El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades", *Manual de las principales novedades del Reglamento Europeo de Protección de Datos,* 2018, Thomson Reuters, p.9.

explicite en el contrato una clasificación de las empresas con las que es posible subcontratar los servicios y los niveles de calidad y seguridad exigidos, según el tipo de actividad subcontratada. De igual forma, un sistema especialmente garantista sería establecer por el encargado del tratamiento de datos, a disposición del responsable del tratamiento, un listado actualizado de empresas con las que se puede subcontratar el servicio, estableciendo la posibilidad de que el responsable del tratamiento pueda mantener o rescindir el contrato según las empresas incorporadas o salientes.

La Agencia Española de Protección de Datos[322] viene a indicar que siempre que el cliente del servicio de *cloud* tenga un conocimiento exacto de la identidad de los terceros subcontratistas del servicio, así como de las actividades desplegadas por cada uno de los subcontratistas, nada obsta a que la subcontratación se realice mediante un único contrato. Por lo tanto, sería suficiente con acreditar la existencia de las garantías adecuadas, citando como ejemplos la puesta a disposición de un sitio web que haga referencia expresa al contrato firmado, los datos de identificación de los subcontratistas, la ubicación de los mismos y los servicios de tratamiento que desarrollan. Cumpliendo estas exigencias, basta la celebración de un único contrato que cumpliese con los requisitos necesarios.

El Tribunal Supremo[323], en 2010, ya se pronunció al respecto indicando que:

> *"... es obligado indicar, contrariamente a lo que sostiene el Abogado del Estado, que aunque el artículo 21 no contiene una previsión específica sobre la facultad del responsable del tratamiento en orden a la comunicación de subcontratación, es claro que esa comunicación del encargado del tratamiento constituye en realidad una propuesta que puede ser rechazada por aquel, bien por entender improcedente la subcontratación, bien por considerar inidónea la empresa con la que se pretende subcontratar. Así se infiere de la capacidad de decisión del responsable del tratamiento y de la responsabilidad que le corresponde.*
>
> *Si el responsable del tratamiento, de conformidad con el artículo 17.2 de la Directiva, debe elegir un encargado del tratamiento que ofrezca garantías suficientes en relación con las medidas de seguridad técnica y de organización de*

[322] Agencia Española de Protección de Datos: "Informe 0157/2012", 2012.

[323] Sentencia del Tribunal Supremo 4050/2010, del 15 de julio de 2010, F.J. décimo. Accesible en: http://www.poderjudicial.es/search/documento/TS/5698482/proteccion%20de%20datos%20de%20caracter%20personal/20100812. Último acceso: 08.08.2018.

los tratamientos que deben efectuarse, y asegurarse que se cumplen dichas medidas, y si de conformidad con el apartado 3 del indicado artículo el encargado del tratamiento solo actúa siguiendo instrucciones del responsable del tratamiento, negar capacidad de disposición a este en supuestos de subcontratación es una conclusión reñida con los más elementales criterios de la lógica".

Un marco de referencia puede ser las garantías establecidas por las cláusulas contractuales tipo de la Decisión de la Comisión Europea 2010/87/UE de 5 de febrero, relativa a las cláusulas contractuales tipo para las transferencias de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo[324]. El principal problema que plantea es el ámbito de aplicación de la citada Decisión, limitándose a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país[325]. Fuera de este ámbito, como indica MARZO PORTERA[326], los Estados Miembros son libres de delimitar las cláusulas tipo establecidas en la Decisión a los responsables del fichero, establecidos en la Unión Europea, cuando proceda a la subcontratación con un prestador de servicios de

[324] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32010D0087. Último acceso: 08.08.2018.

[325] El Grupo de Trabajo del Artículo 29 ha estudiado los instrumentos jurídicos existentes para las transferencias de datos entre un responsable establecido en el EEE y un encargado establecido en el EEE que posteriormente subencarga el tratamiento a un proveedor en un tercer país. GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC", 2010, 00070/2010/EN WP176 (12.07.2010), p. 4. Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf. Último acceso: 08.08.2018.

GUASH PORTAS y SOLER FUENSANTA resume las tres soluciones jurídicas en:

- Contrato directo entre el responsable del tratamiento y el subencargado establecido fuera del EEE. Conforme a la Decisión 2010/87/UE
- Mandato expreso al encargado del tratamiento para poder utilizar las cláusulas contenidas en la Decisión 2010/87/UE.
- Un contrato *ad hoc*.

GUASH PORTAS, Vicente y SOLER FUENSANTA, José Ramón: ""Cloud computing": cláusulas contractuales y reglas corporativas vinculantes", *Revista de Derecho UNED*, 2014, núm. 14, p. 260. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/13300. Último acceso: 08.08.2018.

[326] MARZO PORTERA, Ana María: "Privacidad y cloud computing, hacia dónde camina Europa". *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, 2012, nº 8, p. 216.

un tercer país[327]. Al igual que la Directiva 95/46/CE, la Decisión de la Comisión de 5 de febrero de 2010 establece en su considerando (4) que tanto el exportador como importador de datos tienen plena libertad para incluir cualquier cláusula en el contrato sobre cuestiones relacionadas con sus negocios que consideren pertinentes, siempre y cuando no contravengan las cláusulas tipo de la Decisión, garantes de una correcta protección de datos. En el próximo subapartado se estudiarán de manera detallada las transferencias internacionales de datos personales, particularmente respecto al modelo de la nube.

No se hace referencia, sin embargo, a la necesaria comunicación a los interesados, titulares de los datos, que no tienen por qué coincidir con el cliente en el contrato de la nube. Como recalca FERNÁNDEZ ALLER[328], *"sin control, sin conocimiento de lo que sucede con los datos personales, no hay derecho de autodeterminación informativa"*. La indefensión en que podría caer el titular de los datos en la subcontratación puede ser solventada con una interpretación amplia de los artículos 5, 12.1, 12.3 y 34 del RGPD. La necesidad de que los datos personales sean tratados de manera *"lícita, leal y transparente en relación con el interesado"* debiendo el responsable del tratamiento tomar *"las medidas oportunas para facilitar al interesado toda la información"* sobre los datos personales tratados, así como toda la información relativa al tratamiento, deben remitir a una efectiva comunicación al titular de los datos. Más, conociendo los riesgos que entraña la subcontratación, y cómo el nuevo marco europeo establece en el artículo 34 la comunicación al interesado cuando sea probable una violación de la seguridad de los datos personales.

En otro orden, el Reglamento europeo dictamina, en el artículo 28.3, la obligación expresa de que en el contrato o acto jurídico celebrado entre el responsable y el encargado del tratamiento se recojan las instrucciones documentadas[329], *"inclusive con respecto a*

---

[327] En todo caso, habrá que respetar la normativa protectora de los datos personales, aplicables a responsables y encargados dentro del EEE, limitándose las posibilidades del libre pacto a las materias abiertas a la autonomía contractual.

[328] FERNÁNDEZ ALLER, Celia: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)", *Revista de Derecho UNED*, 2012, núm. 10, p. 139. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/11093/10621. Último acceso: 08.08.2018.

[329] Se ha de recordar, como se ha puesto de manifiesto en el Capítulo III.b.b y Capítulo IV.a, a tenor de los dictámenes del Grupo de Trabajo del artículo 29, que cuando el encargado del tratamiento de la nube, proveedor del *cloud*, no se atenga a las instrucciones del cliente será considerado responsable del tratamiento, debiendo el prestador del servicio informar de todos los subcontratistas que prestan algún

las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público". No solo se queda aquí, en el apartado 2 establece que el encargado del tratamiento no podrá subcontratar parte del servicio *"sin la autorización previa por escrito, específica o general, del responsable"*, delimitando que cualquier cambio en los subcontratistas debe ser informado al responsable de datos para que pueda oponerse a los mismos. La regulación refuerza las directrices marcadas por la Agencia Española de Protección de Datos, *ad supra*, no solo porque el ámbito de aplicación es más amplio, al no limitarse a transferencias internacionales, sino porque otorga al responsable la posibilidad de oponerse a los cambios ejecutados por el encargado, acorde con la postura de nuestro alto tribunal.

La nube, como otros productos informáticos, peca de la pérdida de control de los datos cuando se contratan los servicios, como en reiteradas ocasiones se ha puesto de manifiesto en el presente trabajo. El Reglamento europeo introduce una novedad tendente a compartir la responsabilidad, por la pérdida de control de los datos, entre los sujetos intervinientes en el desarrollo de la actividad. De esta forma, cuando se produzca una subcontratación en el tratamiento de datos, el subcontratista tendrá las mismas obligaciones que las estipuladas en el contrato originario entre el cliente y el proveedor de la nube[330]. Ante el incumplimiento del subencargado, el encargado será responsable

servicio en la actividad, sobre las medidas técnicas de seguridad y los posibles lugares donde se encuentren almacenados los datos. Principalmente se trata el asunto en el Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012.

[330] Conviene recodar, aunque sea someramente, la doctrina general sobre el subcontrato. Declara, nuestro Tribunal Supremo en la Sentencia de 31 de diciembre de 2002, número de resolución 1280/2002, en su FJ III: *"el subcontrato constituye un contrato independiente y autónomo, que genera relaciones jurídicas entre las partes que en ellos intervienen, el subcontratante y subcontratista"*, (accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=3243497&links=%221280%2F2002%22&optimize=20030703&publicinterface=true. Último acceso: 08.08.2018) aclarando que, en Sentencia de 27 de noviembre de 2003, número de resolución 1105/2003, FJ III, *"permanecen subsistentes las relaciones entre las partes que han concertado el llamado contrato padre o básico, de tal modo que quien es parte en el contrato base y a su vez en el subcontrato, conserva tanto la gama de derechos y obligaciones derivadas del primero a la vez que asume los que creó con su subcontratante, resultando así una duplicidad de relaciones"* (accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2806722&links=%221105%2F2003%22&optimize=20040124&publicinterface=true. Último acceso: 08.08.2018).

frente al cliente[331]. El RGPD supone una evolución en la regulación de la subcontratación del tratamiento de datos, en tanto que clarifica la compleja red de relaciones en la subcontratación del servicio. Baste recordar que FERNÁNDEZ ALLER, bajo el paraguas de la LOPD, consideraba que el subcontratista debe considerarse encargado del tratamiento, siendo de aplicación al sujeto el artículo 20.3 del RLOPD[332]. Interpretación que podría generar problemas en ámbitos tan importantes como la responsabilidad del encargado del tratamiento, parte que realiza la contratación, que quedaría excluida del marco normativo.

La posibilidad de establecer cláusulas tipo para reglamentar las subcontrataciones del tratamiento se recogen en los artículos 28.6, .7 y .8 del RGPD.

Por último, se han de citar las restantes exigencias, ya tratadas, que establecía el artículo 21.2 del RLOPD entre el contratista y subcontratista: en primer lugar, que el subcontratista se ajuste a las instrucciones del responsable del fichero; y, en segundo lugar, que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, exigencias que mantiene el RGPD. La AEPD[333], incluso antes de la aprobación del

---

El contratista, obligado principal, puede cumplir la prestación por medio de otra persona, en base al principio de autonomía de la voluntad, para el cumplimiento de la obligación contraída con el contratante. Sin embargo, esta circunstancia no implica que el subcontratista responda exclusivamente por el incumplimiento contractual en el desarrollo material del objeto. Por lo tanto, las relaciones y responsabilidades entre contratante y contratista no se modifican por motivo de la subcontratación. Para que la subcontratación exonere de responsabilidad al contratista deberá pactarse expresamente, aunque no siempre se suficiente (véase la Sentencia del Tribunal Supremo de 3 de abril de 2016, número de resolución 337/2006).

[331] Artículo 28.4 del RGPD: *"Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado"*.

[332] FERNÁNDEZ ALLER, Celia: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)", *Revista de Derecho UNED*, 2012, núm. 10, p. 137. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/11093/10621. Último acceso: 08.08.2018.

[333] AEPD: "Recomendaciones referentes al Plan de Inspección de Oficio a las empresas participantes en la elaboración de los Censos de Población y Viviendas del año 2001", 2003 (17.07.2003). Estas recomendaciones han servido de base para los posteriores informes 582/2004 y 8/2006.

Reglamento de desarrollo (RLOPD), ya manifestaba la necesidad de estos tres requisitos acumulativos para la correcta subcontratación, que implica tratamiento de datos: "*por otro lado, de preverse o producirse por parte del prestador de un servicio una subcontratación que implique tratamiento de datos personales deberá reflejarse en el contrato los requisitos exigidos por la normativa de protección de datos haciendo constar expresamente, además de las prescripciones del citado artículo 12* (LOPD) *que, o bien el contratista del servicio actúa en nombre y por cuenta del responsable del fichero o tratamiento o, alternativamente, se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato: a) Que los servicios a subcontratar se hayan previsto expresamente en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento. b) Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato. c) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero".*

c. Transferencia internacional de datos personales.

En un estudio de DLA Piper UK LLP para la Comisión Europea[334] se concluye que si bien los países objeto de la investigación, miembros de la Unión Europea, conocen las restricciones y prohibiciones que la normativa establece para las transferencias de datos personales fuera del Espacio Económico Europeo, y a pesar de ser frecuente el empleo de cláusulas tipo para las transferencias, ya sean por separado o dentro del contrato de computación en la nube, debido a la naturaleza del servicio las normas de protección de datos actuales son inadecuadas para satisfacer plenamente las obligaciones al respecto.

La contratación de los servicios de *cloud computing* incide, por la naturaleza del servicio, en la problemática de las transferencias internacionales de datos personales y su adecuación con la normativa de aplicación. RUBÍ NAVARRETE[335] parte del deber de diligencia, previo a la celebración del contrato de *cloud computing*, del encargado del tratamiento y del propio responsable, en solicitar la información y ofrecerla, aclarando cuáles serán las garantías que se prestarán si dichas transferencias internacionales se

[334] DLA PIPER UK LLP - COMISIÓN EUROPEA: "Comparative study on cloud computing contracts", 2015, p.40. Accesible en: http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/. Último acceso: 08.08.2018.

[335] RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012, p. 97.

realizan a países que no tengan un nivel adecuado de protección. Este deber inicial es esencial para la correcta protección de los datos personales de los interesados, sin el cual las medidas protectoras que establece la normativa decaerían por insuficientes. Así lo estima, también, el nuevo Reglamento europeo de protección de datos, como se ha reseñado *ad supra*.

El concepto de transferencia internacional se delimita en el artículo 5.1.s) del RLOPD[336]. Se desarrolla un concepto de transferencia que supone cualquier acto de acceso a los datos personales del exportador de datos por el importador, siempre y cuando la transmisión se realice fuera del Espacio Económico Europeo, al haber armonizado estos Estados su derecho nacional conforme a la Directiva 95/46/CE. Sin embargo, ÁLVAREZ RIGAUDIAS[337], a tenor de la jurisprudencia europea, considera que la transferencia de datos personales puede definirse *"como el acto por el cual el transmitente (exportador) permite el conocimiento de los datos personales al destinatario (importador) de forma directa, implicando por tanto una comunicación material de datos personales, con independencia de su finalidad",* a lo que habría que añadir el carácter internacional cuando se localice en un territorio fuera del Espacio Económico Europeo.

El artículo 45 del RGPD, al enunciar las transferencias basadas en una decisión de adecuación, determina que las transferencias de datos personales que se realicen a un tercer país u organización internacional podrán efectuarse cuando la Comisión haya decidido que *"el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado"*, no requiriendo una autorización específica para su transferencia. Será la Comisión, por tanto, la que decida por cualquier acto de ejecución, con efecto para toda la Unión Europea, qué tercer país, territorio, sectores específicos de ese tercer país u organización serán considerados con nivel adecuado de protección.

---

[336] Artículo 5.1.s) del RLOPD: *"Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español."*.

[337] ÁLVAREZ RIGAUDIAS, Cecilia: "Condiciones para las transferencias internacionales de datos personales en servicios de cloud". *Derecho y cloud computing*, 2012, p. 114.

En este sentido, en virtud del artículo 45.4[338] y .9[339] del RGPD, hasta que sean modificadas o derogadas, permanecerán en vigor las decisiones adoptadas al amparo de la Directiva 95/46/CE.

El artículo 26.2 de la Directiva 95/46/CE se encargaba de exceptuar la prohibición de transferencia de datos personales a terceros países, es decir, recoge la posibilidad de autorizar la transferencia de datos personales a un tercer país que no garantice el nivel de protección conforme al artículo 25.2[340], *"cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas"*.

El RGPD, en el artículo 46, contempla la posibilidad de realizar transferencias internacionales a países que no ofrecen un nivel equiparable de protección siempre que se realicen mediante las garantías adecuadas y, como señala GUASCH PORTAS[341], *"a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas"*. Entre los instrumentos que otorgan las garantías adecuadas que permiten las transferencias sin necesidad de autorización expresa de la autoridad de control están las *"cláusulas tipo de protección de datos adoptadas por la Comisión"* y las *"cláusulas tipo*

[338] *"La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE".*

[339] *"Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo"*.

[340] Artículo 25.2 de la Directiva 95/46/CE: *"El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

[341] GUASCH PORTAS, Vicente: "La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE", *Revista de Derecho UNED*, 2017, nº 20, p. 339.

de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión"[342].

La disposición contenida en el artículo 26.2 de la Directiva 95/46/CE se traspone en nuestro ordenamiento en el artículo 70.2 del RLOPD[343]. A falta de la nueva normativa estatal sobre protección de datos personales, debe considerarse de aplicación el Real Decreto. Dos son, consecuentemente, los instrumentos que ofrecen garantías en la transferencia de datos personales a terceros países:

- Contrato entre importador y exportador donde se respete la protección de la vida privada de los afectados y sus derechos y libertades fundamentales, salvaguardando el ejercicio de sus respectivos derechos.
- Contratos respetando lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001 y 2004/915/CE, de 27 de diciembre de 2004, previstas para transferencias internacionales de datos entre responsables del tratamiento; y la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010, cuando la transferencia internacional de datos se produce de un responsable a un encargado del tratamiento.

FERNÁNDEZ ALLER[344] a las dos vías anteriores añadía, como posteriormente reconocerá el vigente RGPD, las transferencias que se producen en el seno de grupos

[342] Por la relevancia práctica de los instrumentos considerados con garantías adecuadas para las transferencias internacionales, que no requerirán autorización expresa de la autoridad de control, reproducimos el artículo 46.2 del RGPD:

"a)un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b)normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados".

[343] Recordar que el artículo 70.1 del RLOPD dictamina que *"cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos"*.

[344] FERNÁNDEZ ALLER, Celia: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)", *Revista de Derecho UNED*, 2012,

multinacionales, como Normas Corporativas Vinculantes (NCV, BCR o, en palabras de la AEPD, Normas Empresariales Vinculantes). Para esta investigadora las BCR *"son un intento de responder a la indeterminación que sobre algunos de estos elementos ha propiciado la evolución de los flujos internacionales de datos, ofreciendo instrumentos que permiten gestionar transferencias a una pluralidad de destinatarios siempre que se encuentren en un mismo grupo y estén ligados por reglas comunes de protección"*[345]. El RGPD, partiendo de la definición establecida en el artículo 4.20[346], establece que las NCV ofrecen las garantías adecuadas para la realización de las transferencias internacionales de datos siempre que reúnan las prerrogativas que dicta el artículo 47.1 del RGPD (sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros; y confieran expresamente a los interesados derechos exigibles referentes al tratamiento de datos personales) y cumplan, como mínimo, con los elementos recogidos en el artículo 47.2. En tal supuesto, la autoridad de control aprobará las NCV conforme al mecanismo del artículo 63[347].

Por otra parte, con la entrada en vigor del RGPD se ha solventado la problemática existente entre las directrices que se recogían en el artículo 26.4 de la Directiva 95/46/CE y su deficiente trasposición en el artículo 34.k de la LOPD. La excepción a la autorización de la AEPD que establecía la LOPD hacía referencia a Estados (*"… como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado."*) y no a contratos de nivel adecuado, por lo que la concurrencia de un contrato redactado conforme a las cláusulas tipo por la

núm. 10, p. 140. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/11093/10621. Último acceso: 08.08.2018.

[345] Aspecto ya tratado en el Capítulo III.b y al inicio del presente, en ocasión del estudio del Grupo de Trabajo del Artículo 29 en su Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012.

[346] *"Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta".*

[347] El Grupo de Trabajo del artículo 29 trató esta temática en "Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 2012, 00930/12/EN WP 195 (06.06.2012)", 2012. Accesible en: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49726. Último acceso: 08.08.2018.

Comisión no eximían de la obligación anteriormente citada. Esta crítica también fue exteriorizada por ÁLVAREZ RIGAUDIAS[348]. Nos trasladaba que la regulación contenida en la norma patria se separaba de lo que dictaba el artículo 26.4 de la Directiva. Esta establecía que las cláusulas contractuales tipos ofrecen las garantías necesarias conforme al artículo 26.2, anteriormente citado, debiendo los Estados Miembros adoptar las medidas necesarias para ajustarse al precepto. Con estas precisiones, por tanto, la AEPD debía autorizar de manera automática toda transferencia internacional basada en un contrato que incorpore las cláusulas tipo. En caso contrario, entraría en contradicción la LOPD con la normativa europea.

El nuevo RGPD incorpora, además, la facultad de adoptar las cláusulas contractuales tipo aprobadas por una autoridad de control, en España la AEPD, cuando sean aprobadas por la Comisión. La adopción de las cláusulas cumplirá con los criterios garantistas del RGPD, eximiendo de la autorización expresa de la autoridad de control para la transferencia internacional. Hasta la fecha la AEPD no ha elevado para su aprobación ningún marco de cláusulas contractuales tipo, si bien, en la resolución del expediente TI/00126/2012 elaboró un conjunto de cláusulas contractuales tipo para autorizar las transferencias internacionales de datos entre un exportador de datos ubicado en España y un importador de datos ubicado en un país que no garantiza un nivel adecuado de protección.

En última instancia cabría, según el considerando del artículo 46.3.a del RGPD, la adopción de *"cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional"*, si bien requerirán la autorización expresa de la AEPD, con los consiguientes costos vinculados a la realización del trámite previo.

Hemos intentado poner de manifiesto que, con la vigencia del RGPD, las transferencias internacionales de datos, siempre que reúnan las garantías adecuadas conforme al artículo 46.2, no requerirán ningún requisito adicional. Por lo tanto, no será necesaria la autorización expresa de la AEPD, en el caso de España, cuando las

[348] ÁLVAREZ RIGAUDIAS, Cecilia: "Condiciones para las transferencias internacionales de datos personales en servicios de cloud". *Derecho y cloud computing*, 2012, p. 120.

transferencias se produzcan al amparo de las cláusulas tipo aprobadas por la Comisión, o sean producto de las NCV, principalmente[349].

Fuera de los supuestos señalados (*"en ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46"*), solo será posible la transferencia internacional de datos cuando *"no* (sea) *repetitiva,* (afecte) *solo a un número limitado de interesados,* (sea) *necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado"*, siempre que el responsable del tratamiento evalúe todos los intereses en juego y se ofrezcan medidas para garantizar la protección de los datos personales[350].

Centrándonos en las transferencias internacionales de datos más comunes en el entorno de la nube, al considerarse al prestador de servicios de computación en la nube encargado del tratamiento, la Decisión 2010/87/UE, que deroga a la Decisión 2002/16/CE, sería de aplicación ante este supuesto de hecho. Delimitado el ámbito de aplicación, encargado y subcontratista deben encontrarse en un tercer Estado. El considerando (23) establece directamente que *"no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento en un tercer país"*. Existe, por lo tanto, libertad en los Estados Miembros para considerar que los principios y garantías de las cláusulas contractuales tipo prestan la adecuada protección a los derechos de los interesados cuando las partes en la subcontratación no se encuentran localizadas en un tercer Estado.

Haciendo acopio de toda la regulación, referenciada someramente, la AEPD puede establecer los instrumentos contractuales que considere garantes de los derechos de los interesados, conforme al artículo 33 de la LOPD y los actuales artículos 46, 47 y 49 del RGPD, pudiendo servirse de las cláusulas contractuales tipo establecidas en la Decisión 2010/87/UE para regular las transferencias internacionales de datos cuando no concurra

[349] Aunque el RGPD establece la excepción de autorización expresa de las autoridades de control para los códigos de conducta y los mecanismos de certificación, artículos 46.2.e y .f, hasta la fecha son instrumentos que no se han desarrollado en la práctica.

[350] El artículo 49.1 del RGPD establece las condiciones que, si se cumple alguna, podría dar lugar a la transferencia internacional.

que encargado y subcontratista se localicen en un tercer país. De igual forma, cuando el supuesto de hecho entre dentro del ámbito de aplicación de la Decisión 2010/87/UE, la AEPD se encuentra obligada a autorizar automáticamente la transferencia internacional de datos si se recogen las cláusulas tipo establecidas en la mencionada Decisión. No cabe lugar a dudas, así lo disponen los artículo 46.2.c) y .d) del RGPD.

La Decisión insta a que las cláusulas contractuales tipo sean firmadas por la entidad exportadora y la entidad importadora, estableciéndose en la Cláusula 11 la posibilidad de autorizar la subcontratación posterior por el importador. El Considerando 23, estudiado por BLANCO ANTÓN[351], permite a las autoridades nacionales adecuar las cláusulas contractuales tipo, con el fin de ofrecer la misma flexibilidad en la subcontratación a los encargados nacionales. Este criterio no se ha adoptado en España, como anteriormente se ha expuesto, al ser necesaria la autorización de la Agencia Española de Protección de Datos.

Las obligaciones del exportador de datos se recogen en la cláusula 4 de la Decisión. De manera sucinta pueden indicarse las siguientes:

- Garantizar que la transferencia y el efectivo tratamiento de los datos personales se han realizado conforme a la normativa aplicable de protección de datos. Incluye la obligación de obtener la autorización del órgano de control del Estado Miembro donde tenga el establecimiento el exportador de datos, cuando fuere necesario.
- Prestar instrucciones al importador de datos, previa y durante toda la relación contractual, para que el tratamiento de los datos personales exportados se realice en nombre del exportador de datos, conforme con la normativa de protección de datos aplicable.
- Exigir al importador medidas técnicas y organizativas específicas mediante un anexo al contrato.
- Verificar que las medidas de seguridad y de organización son suficientes, en función del estado de la técnica y del coste de la aplicación, para proteger los datos de la destrucción accidental o ilícita, de una pérdida accidental, o de

[351] BLANCO ANTÓN, María José: "Transferencia Internacional de Datos Personales", *Actualidad jurídica Aranzadi*, 2012, nº 836, cara.

una alteración, divulgación o acceso no autorizado, según la normativa aplicable.

- Verificar que las medidas de seguridad y de organización efectivamente se llevan a la práctica.
- Para transferencias de datos personales de carácter especial, comunicar a los interesados que los datos son transferidos a un tercer país que puede no satisfacer las medidas de protección establecidas en la Directiva 95/46/CE. Con la entrada en vigor del RGPD, se debe entender que debe satisfacer las medidas de protección de datos personales que establece esta normativa europea.
- Cuando lo solicitaren los interesados, proporcionarles copia de las cláusulas y medidas de seguridad, así como de los subcontratos realizados para la prestación del servicio por los encargados del tratamiento, pudiendo eliminarse las cláusulas puramente comerciales.
- Supervisar que todos los subencargados del tratamiento desarrollan su actividad con el mismo nivel de protección, al menos, que el responsable de los datos, protegiendo sus derechos inherentes.

Las principales obligaciones del importador de datos, recogidas en la cláusula 5 de la Decisión, son:

- El tratamiento de datos personales debe efectuarse exclusivamente en nombre del exportador de datos, de acuerdo con las cláusulas establecidas y las instrucciones dadas. En el supuesto de que ello no fuere posible, se debe informar inmediatamente al exportador, teniendo este la facultad de suspender la transferencia o rescindir el contrato.
- Garantizar que ha adoptado y ejecutado las medidas de seguridad técnicas y organizativas acordadas con el exportador de datos.
- Atender a las consultas que el exportador realice sobre los datos personales transferidos, según los periodos de tiempos establecidos, así como atender a los dictados de la autoridad de control sobre el tratamiento de los datos personales objeto de transferencia.
- Garantizar que no se tienen motivos para creer que la legislación que le es de aplicación le impide cumplir con las instrucciones del exportador de datos y sus obligaciones a tenor del contrato y que, en caso de modificación de la

legislación que pueda tener un efecto negativo sobre las garantías y obligaciones estipuladas en las cláusulas, notificará al exportador de datos dicho cambio en cuanto tenga conocimiento de él, en cuyo caso estará facultado para suspender la transferencia de los datos o rescindir el contrato.

- Ofrecerá, a petición del exportador de datos, sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, seleccionado por el exportador o por la autoridad de control, si la autoridad de control tiene asumida tal competencia.
- Pondrá a disposición de los interesados, previa petición, una copia de las cláusulas o de cualquier contrato existente para el subtratamiento de los datos, proporcionando una descripción sumaria de las medidas de seguridad en aquellos casos en que el interesado no pueda obtenerlas directamente del exportador de datos.
- Garantizar que en la subcontratación del tratamiento de datos se ha informado, previamente, al exportador de datos, habiendo obtenido para dicha subcontratación su consentimiento previo por escrito.

Dentro de este elenco de obligaciones deben diferenciarse, siguiendo a NAVAS NAVARRO[352], las obligaciones materiales y las obligaciones de garantía. En lo concerniente a las segundas, se establece la obligación notificar al exportador *"toda solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de ley a menos que esté prohibido"*, el acceso fortuito o no autorizado y las solicitudes sin respuesta de los terceros[353]; la obligación de tratar las *"consultas del exportador de datos relacionadas con el tratamiento que este realice de los datos personales sujetos a transferencia"*, así como la obligación de atender *"a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos"*; la obligación de suministrar copias de los contratos de subcontratación que requieran el acceso a los datos, eliminando la información comercial si la tuviera y sin

[352] NAVAS NAVARRO, Susana: "Computación en la nube: Big Data y protección de datos personales", *InDret,* 2015, vol. 4, p. 38-39. Accesible en: http://www.indret.com/pdf/1193_es.pdf. Último acceso: 08.08.2018.

[353] Supuestos de especial relevancia ante normas de diferentes Estados que interfieren en la privacidad y la seguridad de los datos en la nube, sirva de ejemplo la CLOUD ACT anteriormente reseñada.

detalle completo de las medidas de seguridad implementadas; y la obligación de enviar sin demora al exportador de datos una copia de cualquier acuerdo con el subencargado del tratamiento que concluya, con arreglo a las cláusulas establecidas.

El régimen de responsabilidad se encuentra prescrito en la cláusula 6. Destaca, en referencia a las partes del contrato, cliente y prestador de servicios, que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones contractuales por cualquier subencargado del tratamiento tendrán derecho a percibir una indemnización del exportador de datos por el daño sufrido. Añade que el importador de datos no podrá eludir sus responsabilidades en base al incumplimiento de un subencargado del tratamiento. El régimen se completa con una prerrogativa al interesado afectado: si este no pudiera interponer contra el exportador de datos la demanda de indemnización por incumplimiento del importador de datos o su subencargado del tratamiento – por haber desaparecido de facto, cesado de existir jurídicamente o ser insolvente – el importador de datos acepta que el interesado pueda demandarle a él en lugar del exportador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos contractualmente o por ministerio de la ley. Dicha responsabilidad se reproduce en el apartado 3 respecto al subencargado del tratamiento, en cuanto a sus propias operaciones de tratamiento de datos, cuando no sea posible interponer demanda contra el exportador de datos o el importador de datos.

En referencia a la jurisdicción y legislación aplicable, las cláusulas 7 y 9 establecen que el interesado tiene la facultad de someter el conflicto, para la protección de sus derechos o para la reclamación por daños y perjuicios, a mediación por una persona independiente o autoridad de control, si procede, o ante los tribunales del Estado Miembro de establecimiento del exportador de datos. Ello no puede obstaculizar los derechos sustantivos o procedimentales que le correspondiere al interesado de conformidad con el Derecho nacional o internacional. La Decisión determina, igualmente, que la legislación aplicable se corresponderá con la del Estado Miembro de establecimiento del exportador de datos.

En este estudio de las cláusulas de la Decisión 2010/87/UE cabe reseñar, por último, las obligaciones una vez finalizada la prestación de los servicios de tratamientos de datos personales. La cláusula 12 compele que, finalizada la prestación de servicios, el exportador determinará, a su elección, que el importador y el subencargardo de

tratamiento de datos devuelvan todos los datos personales transferidos y sus copias, o se destruyan por completo los datos tratados, debiendo certificar esta circunstancia al exportador. Dicha medida se exceptuará si la legislación aplicable impide al importador devolver o destruir los datos personales. En tal supuesto, se garantizará el secreto de los datos personales, además del compromiso de no volver a tratar los datos transferidos. Como garantía se faculta al exportador o a la autoridad de control, bajo petición expresa, auditar las instalaciones de tratamiento del importador de datos y del subencargado del tratamiento.

La AEPD[354] ha dictaminado que las modificaciones de las cláusulas tipo de la Decisión 2010/87/UE alteran las garantías para las transferencias internacionales de datos derivadas de la contratación del servicio de computación en la nube cubiertas por la Decisión, al no ser el modelo estandarizado adoptado por la Comisión. Por lo tanto, no cabría amparar la autorización de la transferencia internacional de datos en la Decisión 2010/87/UE, si bien, pueden ser consideradas conforme a la normativa de protección de datos de carácter personal conforme al artículo 26.2 de la Directiva 95/46/CE y al artículo 70.2 del RLOPD si se salvaguarda la existencia de las garantías adecuadas exigidas por la LOPD, extensible si cumple con las exigencias del RGPD. Por lo tanto, y recogiendo expresamente las consideraciones del informe 0157/2012 de la Agencia Española de Protección de Datos, si se *"adoptase unas cláusulas estandarizadas que aun difiriendo de las contenidas en la Decisión 2010/87/CE contuviesen las garantías adecuadas de protección de los derechos de los afectados y, en particular, de su derecho fundamental a la protección de datos, aun no incluyendo previsiones tales como las relativas a la totalidad de los detalles exigidos en el Apéndice 1 de las cláusulas o introduciendo modificaciones en el tenor de algunas de las cláusulas, …, sería posible que por parte de esta Agencia se dictase resolución determinando que las garantías contenidas en las citadas cláusulas deben considerarse adecuadas a los efectos previstos en el artículo 33.1 de la Ley Orgánica 15/1999, lo que implicaría una autorización automática de cualquier transferencia internacional realizada al amparo de tales cláusulas en tanto no se produjera ninguna alteración de las mismas".* La propia Agencia elaboró, como ya se ha indicado, un conjunto de cláusulas contractuales tipo, similares a las establecidas por la Comisión, con el fin de autorizar las transferencias internacionales de datos y las posibles

[354] AEPD: "Informe 0157/2012", 2012.

subcontrataciones, en la resolución del expediente número TI/00126/2012[355], pero no están aprobadas por la Comisión. Ante este supuesto, deberá constar necesariamente la autorización para la subcontratación.

Para finalizar, no debe olvidarse que siempre que las transferencias de datos tengan como destino un país con un nivel adecuado de protección[356] deberá redactarse un contrato de prestación de servicios entre el responsable y el encargado del tratamiento *"u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros"*, conforme al artículo 28 del RGPD, al igual que establecía el artículo 12 de la LOPD, y los artículos 20 a 22 del RLOPD, siendo necesario que, cuando aparezcan subencargados, las garantías de protección se mantengan, siendo necesaria la autorización del responsable, o en el menor de los supuesto, su conocimiento. En este orden, el Tribunal Europeo de Justicia, el 6 de octubre de 2015[357], invalidó la decisión de la Comisión de considerar a las entidades estadounidenses adheridas al *Safe Harbor* como nivel adecuado de protección en materias de protección de datos. Con estos acuerdos, solo era necesario la realización de un contrato de prestación de servicios conforme a la normativa indicada, sin requerir la autorización de la AEPD. Con el *"Safe Harbor 2.0"*, llamado *EU-U.S. Privacy Shield*, aprobado el 12 de julo de 2016, se permite, de nuevo, realizar transferencias internacionales de datos desde los países miembros a los Estados Unidos sin necesidad de abordar la autorización de la entidad de control[358]. Recientemente, los

[355] Resolución de autorización de transferencias internacionales de datos a Perú. Accesible en: http://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/auto_transf_2012/common/pdfs/TI-00126-2012_Resolucion-de-fecha-16-10-2012_de-GLOBAL-SALES-SOLUTIONS-LINE-S.L.-GSS-LINE-c--GLOBAL-SALES-SOLUTIONS-LINE-S.L.-SUCURSAL-EN-PER-UU-_a-Per-uu-.pdf. Último acceso: 24.01.2017.

[356] Puede consultarse los países con un nivel adecuado de protección en el siguiente enlace de la AEPD: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php. Último acceso: 08.08.2018.

[357] Accesible en: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES. Último acceso: 08.08.2018. Un estudio extenso de la Sentencia lo realiza GARCÍA DE PABLOS, Jesús Félix: "La transferencia de datos fuera de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2016, núm. 40, p. 27-49.

[358] Se recomienda hacer una lectura introductoria sobre el *Privacy Shield* de RAMOS SUÁREZ, Álvaro: "Novedades de 2016 en materia de Privacidad y Ciberseguridad", *Actualidad Jurídica Aranzadi*, 2016, núm. 923/2016, parte Comentario. Así como el artículo de PAEZ, Mauricio; VON DIEMAR, Undine; LITTLE, Jonathon; ROBERTSON, Elizabeth; BRU, Paloma; HAAS, Olivier; y DE MUYTER, Laurent: ""EU-U.S. Privacy Shield" to replace "Safe Harbor"", *Jones Day Publications*, 2016. Accesible en: http://www.jonesday.com/eu-us-privacy-shield-to-replace-safe-harbor-02-04-2016/. Último acceso: 08.08.2018.

eurodiputados han pedido a la Comisión de la UE que vuelva a suspender el *EU-US Privacy Shield* a menos que, antes del 1 de septiembre de 2018, cumpla con las normas de protección de datos compilada con la Unión[359]. Con el nuevo Reglamento europeo de protección de datos, volvemos a señalizar, se precisa que el proveedor de la nube acredite las medidas de seguridad oportunas, exigiéndose similares garantías tecnológicas para las siguientes subcontrataciones.

d. Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal

El legislador español, para adaptarse a la nueva realidad que impone el RGPD, ha optado por la elaboración de una nueva Ley Orgánica que derogue la conocida LOPD. El 24 de noviembre de 2017, siguiendo el trámite parlamentario oportuno, se publica el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal[360] (PLOPD) con el objetivo de que, antes de la plena vigencia del RGPD, 25 de mayo de 2018, España cuente con el instrumento jurídico oportuno que desarrolle y siente las bases del derecho fundamental a la protección de datos personales. Sin embargo, esta adaptación de las normas nacionales al nuevo RGPD se realizará tarde, por cuanto hasta la fecha continúa tramitándose en el Congreso de los Diputados el Proyecto de Ley. Cerrado el período de enmiendas, se presentaron por los grupos parlamentarios un total de 369 enmiendas[361]. El número de enmiendas parciales presentadas y el juego de las mayorías parlamentarias dificultan este proceso legislativo que ya nació tarde y que, aunque el RGPD sea aplicable directamente, es necesario, y casi diríamos esencial, para que los ciudadanos puedan conocer las disposiciones en materia de protección de datos que resultan aplicables, así como la concreción en aquellos aspectos en los que el RGPD da margen a los Estados para adoptar la regulación más adecuada. Sin embargo, y a pesar de la futura aprobación

[359] PARLAMENTO EUROPEO (Nota de prensa): "Suspend EU-US data exchange deal, unless US complies by 1 September, say MEPs", 2018, nota de 05 de julio de 2018. Accesible en: http://www.europarl.europa.eu/news/es/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps. Último acceso: 08.08.2018.

[360] Accesible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF. Último acceso: 08.08.2018.

[361] Puedes acceder a las enmiendas en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-2.PDF. Último acceso: 08.08.2018.

de la Ley, nos encontraremos, como bien recoge PLAZA PENADÉS[362], con una doble regulación en materia de protección de datos: la futura LOPD y el RGPD[363], con la complejidad que supone y con la prevalencia siempre del Reglamento europeo. En este contexto, sin perjuicio de las posibles modificaciones que pueda sufrir en el trámite parlamentario, queremos reseñar las novedades más importantes que plantea el PLOPD para el entorno de la nube.

El PLOPD aumenta el número de entidades y supuestos en los que será obligatoria la figura del delegado de protección de datos, artículo 34. En particular, destacan a nuestros efectos las entidades que exploten redes y presten servicios de comunicaciones electrónicas cuando de forma habitual y a gran escala traten datos personales; los prestadores de servicio de la sociedad de la información, cuando a gran escala elaboren perfiles de usuarios; las entidades aseguradoras y reaseguradoras; las empresas de los servicios de inversión; las entidades que desarrollen actividades de publicidad y prospección comercial; y los centros sanitarios obligados al mantenimiento del historial clínico de los pacientes. Estas entidades, aun pudiendo pecar de simplista, por su labor empresarial y comercial intercambian un número elevado de datos e información con empresas del grupo y con terceros, principalmente a través de herramientas informáticas como la nube.

Decíamos que el principio de *accountability*, recogido en el RGPD, obligaba al responsable del tratamiento a una evaluación de impacto, artículo 35, bajo una serie de condicionantes[364]. El PLOPD, en el artículo 28, incorpora dentro de las medidas proactivas o de responsabilidad activa la obligación a los responsables y encargados de valorar si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3.ª del Capítulo IV del citado reglamento.

---

[362] PLAZA PENADÉS, Javier: "El Proyecto de la nueva Ley Orgánica de Protección de Datos de Carácter Personal", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* 2018, núm. 46, parte especial. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

[363] Así lo recoge expresamente el artículo 1.2 del PLOPD: *"El derecho fundamental de las personas físicas a la protección de datos de carácter personal, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica".*

[364] En particular, artículo 35.3 del RGPD: *"a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público".*

Además de esta novedad, incorporar de forma clara la obligación del encargado de valorar la necesidad de realizar la evaluación de impacto, añade la realización de la evaluación de impacto cuando se desarrollen actividades que impliquen una evaluación de aspectos personales con la creación o utilización de perfiles personales para el análisis o predicción de su situación económica, solvencia económica, preferencias o intereses, y comportamientos, entre otros. Estas actividades están directamente relacionadas con los supuestos de designación obligatoria del DPD. El legislador está pensando, por tanto, en aquellas actividades comerciales que implican un alto grado de tratamiento de datos y que, en otro orden, han implantado en su desarrollo de negocio herramientas informáticas que permiten un uso colectivo de los datos e información. En el entorno del *cloud,* también tiene especial incidencia la consideración de la evaluación de impacto cuando se produzca un tratamiento masivo que afecte a un gran número de interesados o implique un elevado número de datos personales; cuando sean objeto de transferencia a terceros Estados u organizaciones internacionales, de forma habitual, que no tuvieren declarado un nivel adecuado de protección; o cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad, fraude, pérdidas financieras, daño para la reputación o pérdida de confidencialidad de los datos sujetos al secreto profesional. El PLOPD aclara, desarrolla y complementa la escueta redacción del RGPD.

Se ha indicado que la portabilidad de los datos personales se configura como un derecho para el interesado y, en otra vertiente, como una posibilidad que el cliente (responsable del tratamiento) puede regular en el contrato de computación en la nube. Respecto a esta última opción, el PLOPD recoge que, artículo 4, no será imputable al responsable del tratamiento los datos inexactos obtenidos del interesado directamente por él, de aquellos que se hubiesen obtenido de otro responsable del tratamiento en virtud de la ejecución del interesado del derecho a la portabilidad o cuando hubiere obtenido los datos de un mediador o intermediario si las normas aplicables al sector de la actividad al que pertenezca el responsable del tratamiento establecen tal posibilidad, siempre que se hayan adoptados las medidas razonables para que se supriman o se rectifiquen sin dilación. El legislador nacional consciente de las posibles dificultades que se pueden encontrar los diferentes responsables del tratamiento ante las transferencias de datos por el ejercicio del derecho de portabilidad exime al responsable del tratamiento del *cloud* de las inexactitudes que pudieran producirse en el traspaso.

Esta presentación de las novedades que ostenta el PLOPD no se realiza de forma exhaustiva, solo se ha querido resaltar aquellos aspectos que pueden tener mayor incidencia en el desarrollo de la nube. La inclusión de una casilla específica en el contrato de tratamiento para proceder a la declaración de consentimiento expreso en el tratamiento que exige el RGPD, la edad de 13 años como límite en la que un menor puede prestar consentimiento, el principio de transparencia establecido por capas, las restricciones adicionales en los datos especialmente protegidos, la licitud del tratamiento de datos de contacto sobre las personas físicas que presten servicios en personas jurídicas justificado en el interés legítimo, el ejercicio de los derechos de acceso, rectificación o supresión por los herederos de una persona fallecida siguiendo las instrucciones del finado, o el desarrollo y clarificación de las infracciones y sanciones son las principales aportaciones, en términos generales, del Proyecto.

Habrá que esperar, dada la cantidad de enmiendas presentadas, al documento resultante para determinar la repercusión o influencia de la norma nacional en el derecho fundamental de protección de datos, dentro de las posibilidades que el RGPD reconoce.

CAPÍTULO V – EL CONTRATO DE *CLOUD COMPUTING*. a. La prestación del servicio del *cloud computing* entre empresas: *a. Condiciones generales en el contrato del cloud computing: i. Contratantes, parte expositiva y el objeto del contrato; ii. Obligaciones de las partes; iii. Protección de datos de carácter personal: iv. Duración y terminación del contrato; v. Jurisdicción y ley aplicable. b. Cláusulas específicas en el contrato de cloud computing: i. Responsabilidad, ii. Uso aceptable, iii. Localización y tratamiento de datos, iv. Seguridad en el servicio, v. Lock-in y lock-out, vi. Derechos de Propiedad Intelectual e Industrial, vii. Acuerdos de Nivel de servicio (ANS o SLA), viii. Cambio de las características del servicio y renovación del ANS. c. Epítome sobre la extinción del contrato de computación en la nube entre empresas: causas y efectos de las obligaciones.* **b. La protección del consumidor en el contrato de *cloud computing***: *a. Definición de consumidor a la luz de la normativa aplicable: i. Consumo mixto. b. Cláusulas generales de contratación, cláusulas no negociadas individualmente y cláusulas de protección al consumidor. c. Análisis de las cláusulas contractuales en la prestación del cloud cuando el cliente es un consumidor: i. Protección al consumidor de la nube antes de la perfección del contrato; ii. Ámbito de aplicación; iii: Protección ex post, estudio de las cláusulas contractuales en la contratación con consumidores: a'. Protección de datos, b'. Variación de los términos del contrato, c'. Jurisdicción y sumisión al arbitraje, d'. Ley aplicable, e'. Responsabilidad, f'. Uso aceptable, g'. Localización y tratamiento de datos, h'. Garantías y devolución del crédito por servicios no consumidos, i'. Acuerdos de Nivel de Servicios (ANS o SLA), cambios y renovación, j'. Extinción del contrato*. **c. La contratación del *cloud computing* en el sector público:** *a. El empleo de los medios electrónicos en las Administraciones públicas. Mimbres para la utilización de la nube. b. Tipo contractual del cloud computing según la normativa administrativa. c. Cláusulas necesarias en el contrato administrativo. d. Experiencias de la contratación del cloud computing en el sector público y breves notas sobre la Red SARA: i. La nube para PATRIMONIO NACIONAL, ii. La nube para RED.es, iii. La red SARA para las Administraciones públicas en España.*

CAPÍTULO V – EL CONTRATO DE *CLOUD COMPUTING*

CHOU[365] nos recuerda que toda externalización o contratación externa de los sistemas de información cuenta con tres etapas esenciales: una fase previa al contrato donde se identifican las necesidades de externalización, se planifican y seleccionan las estrategias y se elige al proveedor más oportuno, según nuestras necesidades; una segunda fase contractual, para regular la transición y ejecución de los servicios informáticos; y una última fase pos-contractual donde materialmente se ejecuta el servicio y se evalúa el programa seleccionado. El contrato, por tanto, aparece como la piedra angular en el ciclo de vida de la prestación del servicio informático, moderador de los riesgos y las responsabilidades que previsiblemente aparezcan en el desarrollo del servicio.

En el Capítulo II se ha tratado de forma prolija el contrato informático. La naturaleza del objeto del contrato en nada condiciona el modo de perfección del contrato. Discutíamos si el Derecho informático en su conjunto, y por ende la contratación de la computación en la nube, requiere de la existencia de un área jurídica con autonomía científica que se ocupe de todo lo relacionado con la informática, lo que conllevaría a que los contratos informáticos fueran un tipo especial de contratos, con autonomía jurídica y financiera. Sirva como síntesis la argumentación de MADRID PARRA[366], al establecer que la existencia de una pluralidad de bienes y servicios con similar naturaleza o característica que pueden ser objeto en la contratación, no determina el nacimiento de un nuevo tipo o categoría contractual. En consecuencia, la contratación de servicios informáticos determinará la existencia de cláusulas contractuales específicas, pero nada nuevo añade desde una perspectiva jurídica, aunque a la luz de los medios empleados aparezcan principios jurídicos nuevos como los principios de equivalencia funcional o neutralidad tecnológica, entre otros.

Los contratos de *cloud computing* son, habitualmente, contratos de adhesión, en los que una de las partes fija las cláusulas del contrato y la otra se adhiere, sin posibilidad de modificación. La complejidad del contenido del contrato del *cloud* propicia que una de las partes no cuente con la preparación o los medios suficientes para negociar el contrato,

[365] CHOU, David C.: "Cloud computing risk and audit issues", *Computer Standards & Interfaces*, 2015, núm. 42, p. 138.

[366] MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111, p. 28.

lo que conlleva a que se acepte la oferta sin conocimiento preciso del contenido contractual. DÁVARA RODRÍGUEZ[367] indica que para los servicios informáticos los contratos de adhesión son necesarios, si bien, en ellos se producen frecuentemente situaciones abusivas. Los contratos informáticos tipo en muchas ocasiones provienen de lugares que tienen otros usos o normativas diferentes a la nuestra, principalmente creados al amparo de los sistemas jurídicos de *common law*, exportando cláusulas de dudosa efectividad y validez en nuestro sistema normativo. De estas cláusulas importadas, resulta frecuente encontrar aquellas que exoneran la responsabilidad de los proveedores.

Los clientes requieren mecanismos que les ayuden a evaluar y determinar el significado de los términos, principalmente los relacionados con la seguridad del servicio de la nube, especialmente relevantes ante los cambios que se producen en la ejecución del servicio, exigiendo una evaluación y administración constante. LUNA, SURI, IORGA y KARMEL[368] insisten en que, reforzando la estrategia sobre el *cloud computing* de la Comisión Europea (a través del ETSI, the European Telecommunications Standards Institute), los contratos y los Acuerdos de Nivel de Servicios son los marcos idóneos para conducir la correcta adopción del servicio, para entender lo que hay detrás del servicio de la nube y relacionarlo con nuestros requerimientos. Estos mecanismos pueden ser usados para atraer y dar credibilidad al *cloud*, ayudando a la diferenciación del servicio.

a. La prestación de servicios del *cloud computing* entre empresas

GARCÍA DEL POYO[369] establece que el elemento básico en la prestación de servicios de *cloud computing* a empresas es la elaboración y firma de un contrato entre las partes. La vía contractual, ante la insuficiente regulación en nuestro ordenamiento jurídico, que contemple un clausulado con las especificaciones técnicas del servicio (objeto) y su régimen jurídico aplicable, se configura como solución material en el desarrollo del contrato informático. La complejidad suele ser una característica vinculada a la contratación informática, encontrando su máxima expresión en el entorno del *cloud*,

[367] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 266-268.

[368] LUNA, Jesús; SURI, Neeraj; IORGA, Michaela; y KARMEL, Aniel: "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards", *IEEE Cloud Computing*, 2015, vol. 2, p. 33.

[369] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 59.

por la inmaterialidad del objeto, la reciente instauración del servicio, el lenguaje especializado y los procesos técnicos establecidos[370].

En el ámbito de las relaciones empresariales basadas en la prestación del servicio de la computación en la nube, regirá el principio de libertad de forma, establecido en el artículo 51 del Código de comercio y en los artículos 1.278 y siguientes del Código civil. Siendo el contrato del *cloud* un acto de comercio regulado en el Código de comercio, no cabe duda que debe clasificarse como mercantil[371]. A riesgo de parecer redundante, y siguiendo a GARCÍA DEL POYO[372], el desarrollo de la contratación de los servicios del *cloud* entre empresas, dentro de su ámbito empresarial, supone un acicate más para determinar el carácter mercantil del contrato.

En virtud del negocio jurídico que se establece en el contrato del *cloud*, podría considerarse que la contratación del servicio informático de computación en la nube presumiría la consideración de un contrato de los denominados de resultado. Ello supondría salvaguardar los problemas que plantean el desconocimiento o el difícil conocimiento que los usuarios o clientes del servicio pueden tener de esta tecnología. Sin embargo, DÁVARA RODRÍGUEZ[373] resalta que *"aunque esto, en principio, puede parecer adecuado, y es cierto que se salvarían muchos problemas de los hasta ahora existentes, también es cierto que estaríamos trasladando el problema de una contratación clara y nítida a un arrendamiento de obra, en el que los resultados obtenidos, a la conclusión de la obra, fijarían el cumplimiento de la obligación por una de las partes"*. Es más, la propia naturaleza de la contratación informática impide que se asevere de forma absoluta la teoría del resultado. Por ejemplo, dada la evolución de la tecnología y la complejidad del servicio de la computación en la nube, sería complicado prestar un servicio en nube tipo *SaaS* que no tenga ningún fallo en el desarrollo del servicio o suponga un tratamiento óptimo durante un largo periodo de tiempo. De otra forma,

[370] MADRID PARRA, Agustín: "Los contratos electrónicos y los contratos informáticos", *Revista de Contratación Electrónica*, 2011, nº 111, p. 28.

[371] En el próximo epígrafe, .b, se estudiará la calificación del contrato y la incidencia cuando la contraparte es un consumidor o usuario.

[372] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 60.

[373] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 262-263.

supondría cargar todas las responsabilidades y riesgos sobre el proveedor del *cloud* de forma desproporcionada y discriminatoria.

En la vertiente opuesta se plantea el contrato de la nube como contrato de prestación de servicios. Sin embargo, en la contratación del *cloud computing* el proveedor de servicios no queda comprometido a facilitar una serie de servicios, como objeto de contrato, sino que debe exigírsele algún tipo de resultado. Atendiendo a la naturaleza del servicio pretendido, en la que se destaca la tecnicidad del servicio, parece fundamental establecer una serie de compromisos de resultado. Este razonamiento es esencial para los parámetros de medición y evolución contenidos en los ANS que deben incorporar todos los contratos en la nube. Por lo tanto, parece que la forma más oportuna de definir al contrato de *cloud* es con el término *outsourcing*[374]. Volviendo a DÁVARA RODRÍGUEZ[375], una correcta definición sería *"la cesión de la gestión de los sistemas de información de una entidad a un tercero que, especializado en esta área, se integra en la toma de decisiones y desarrollo de las aplicaciones y actividades propias de la referida gestión, con la finalidad de la optimización de los resultados de la misma, al tiempo que permite a la entidad el acceso a nuevas tecnologías y utilización de recursos especializados de los que no dispone"*. Recoge los caracteres esenciales del servicio del *cloud*, considerando los modelos existentes del servicio, en tanto que cubre el almacenamiento de datos y la gestión de esa información mediante la tecnología contratada, buscando un ahorro en espacio, facilidad de organización, escalabilidad y mejora en la gestión, lo que redundará en una optimización en la gestión y recursos de la empresa[376].

En virtud de lo expuesto, nos encontramos ante un contrato atípico[377] al que, en España, le resultará de aplicación la normativa de carácter general que regula las

[374] En el Capítulo II.a se trata de manera extensa los contratos informáticos y en el apartado .b se desarrolla el concepto de bienes informáticos.

[375] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 278-279.

[376] Para su comprensión, se ha utilizado un concepto amplio de *outsourcing*. Como señaláramos en el Capítulo II.e, la principal diferencia con el contrato tradicional de este servicio informático es que el *cloud computing* permite la posibilidad de compartir el entorno con otros clientes sin necesidad de unos conocimientos elevados del desarrollo tecnológico. Emplazamos, para un estudio completo, al apartado indicado.

[377] En el capítulo II.e considerábamos, por razón del objeto del contrato de la nube, su carácter mixto.

obligaciones y contratos y el principio de la autonomía de la voluntad de los contratantes, es decir, los artículos 50 a 63 del Código de comercio y los artículos 1.088 a 1.314 del Código civil, en lo no cubierto por aquel. Será igualmente de aplicación la normativa específica, que dependerá de la ley aplicable al contrato que se establezca con el proveedor de servicios[378]. Cuando sea de aplicación la normativa española, habrá que atenerse al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su reglamento de desarrollo y el Real Decreto 1720/2007, de 21 de diciembre, dado el intercambio de datos e información que suponen los servicios en *cloud*[379]; la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, por el marco donde se desarrolla la prestación de servicios, la práctica común de realizar estos contratos por vía telemática y la consideración del proveedor de servicios como prestador de servicios de la Sociedad de la Información; y el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia[380], dado que la utilización de obras, *software* o aplicaciones, con sus respectivas protecciones, son parte esencial del

[378] En el Capítulo III.b hemos estudiado los trabajos proporcionados por el Grupo de Trabajo del artículo 29. Aunque posteriormente profundizaremos en la normativa aplicable al contrato de la computación en la nube, el Grupo de Trabajo del artículo 29, en su opinión 5/2012 emitida el 1 de julio de 2012, indica que los criterios para determinar la normativa aplicable están contenidos en el artículo 4 de la Directiva 95/46/CE. En la misma se indica que la legislación aplicable a los servicios del *cloud* será la ley del país en que esté establecido el *controller contracting*, que será el cliente, de la contratación de los servicios del *cloud*, y no el lugar donde operen los proveedores. Si bien, para la aplicación del criterio enunciado, el proveedor de servicios debe establecer uno o más centros dentro del Espacio Económico Europeo (EEE) o, no poseyéndolos, se sirvan de equipos operativos que se ubiquen dentro del EEE. Una reseña más debe destacarse: este Grupo de Trabajo estudia la normativa referente a la protección de datos personales. Especialmente relevante, como señaláramos *ad supra*, es la novedad introducida por el nuevo Reglamento europeo de protección de datos, que en su artículo 3.2 señala como directamente aplicable la nueva normativa de tratamiento de datos personales a los residentes en la Unión *"por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión"*.

[379] Véase el Capítulo IV.b.

[380] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930. Último acceso: 08.08.2018.

desarrollo del servicio del *cloud*. A la fecha, la Comisión Europa está en elaboración y propuesta del Reglamento de la Privacidad y las Comunicaciones Electrónicas[381].

Antes de realizar un estudio pormenorizado de las cláusulas contractuales características del contrato del *cloud computing* y de los anexos más relevantes, es oportuno atender a las fases de la contratación, que por las características propias del objeto modelizan el contrato. En el prefacio del capítulo citábamos a CHOU para sistematizar las principales etapas en toda externalización de servicios. DÁVARA RODRÍGUEZ[382], compartiendo como esenciales las fases expuestas, determina las características especiales de la contratación informática en cada una de ellas:

- La fase precontractual o preliminar es determinante para que la finalidad pretendida con el contrato llegue a materializarse. La probable desigualdad en la formación y capacitación informática entre las partes intervinientes en el contrato, aconsejan el asesoramiento profesional para fijar el contenido y la finalidad del contrato. Este desequilibrio no solo se manifestará en la fase precontractual, sino que se hará visible en el acuerdo de voluntades. Desde esta perspectiva, el asesoramiento externo y previo viene a reestablecer esta desigualdad inicial, propiciando que se sienten las bases de las especificaciones del producto, que orientarán, ya en la fase de contratación, las características del contrato. MADRID PARRA[383] y DÁVARA RODRÍGUEZ[384] recomiendan, dada la complejidad del objeto del contrato, una serie de pactos previos, denominados "declaración de intenciones", que suponen un marco de actuación previo o esbozo del futuro contrato, el cual recogerá los parámetros de partida del contrato definitivo. Aunque suele ser un compromiso para negociaciones futuras, nada impide que se configure como un contrato autónomo en sí. Debe recordarse las implicaciones que

[381] Más información en: http://europa.eu/rapid/press-release_IP-17-16_es.htm. Último acceso: 08.08.2018. La Propuesta del Reglamento de la Privacidad y las Comunicaciones Electrónicas se encuentra en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010. Último acceso: 08.08.2018.

[382] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 281-284.

[383] MADRID PARRA, Agustín: "Los contratos electrónicos y los contratos informáticos", *Revista de Contratación Electrónica*, 2011, nº 111, p. 30-31.

[384] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 282.

tiene el artículo 1.902 del Código civil, si fuere aplicable la normativa española, referente a la responsabilidad por culpa.

- En la perfección del contrato, el acuerdo de voluntades debe establecer la coincidencia del consentimiento sobre el objeto del contrato. En este tipo de contrataciones es de capital importancia una clara redacción y definición del objeto, más si cabe ante las distintas modalidades del *cloud*, con la finalidad de evitar un posible vicio en el consentimiento. Una correcta definición de las fases de aceptación del producto, antes de su recepción definitiva, el momento de entrega, los períodos de prueba o el trabajo en paralelo parecen contenidos capitales. Es fundamental, como posteriormente ahondaremos, en los contratos de computación en la nube determinar cómo se verificará el servicio respecto a las especificaciones preestablecidas. La adecuada ejecución del contrato depende, en gran medida, de la correcta concreción de esta fase.
- En la etapa de desarrollo y ejecución cobra especial importancia las responsabilidades de las partes, delimitada por una correcta definición del objeto del contrato y el negocio jurídico. Son aplicables, por tanto, las normas de saneamiento por evicción y vicios ocultos, que en nuestro Código civil se regulan en los artículos 1.475 a 1.499 y 1.553. Advierte MADRID PARRA[385] que las cláusulas de garantía guardan importancia por las posibles disputas que pueden surgir ante reclamaciones de derechos de propiedad intelectual e industrial, más si cabe cuando se utiliza un modelo tipo *software* en el *cloud*.

Centrándonos en la fase intermedia, pero obrando conforme a las características esenciales de la etapa precontractual y de ejecución del servicio, el contrato de computación en la nube establecido entre empresas se estructura en dos partes claramente diferenciadas: el acuerdo marco, donde se recogen los términos de carácter general que regularán la relación empresarial, y los anexos, de especial importancia en el servicio requerido al recoger las especificaciones y detalles del objeto contractual, marco esencial para garantizar la conveniencia y satisfacción de las necesidades de la empresa que requiere los servicios de *cloud*.

[385] MADRID PARRA, Agustín: "Los contratos electrónicos y los contratos informáticos", *Revista de Contratación Electrónica*, 2011, nº 111, p. 31-32.

Los anexos contienen consideraciones eminentemente técnicas, sin que ello suponga que su contenido sea de menor importancia a lo establecido en el contrato marco, es decir, tienen la misma fuerza de obligar. Podría considerarse, incluso, que, dada la complejidad del servicio del *cloud computing*, se hace necesario detallar el alcance del servicio, siendo este documento el valedor de tales características. Es más, incluso el precio pactado y las condiciones de facturación pactadas por las partes quedarán desglosados y relacionados con las prestaciones pactadas en los anexos al contrato[386]. Dentro de los anexos típicos podemos encontrarnos los procedimientos a seguir para los servicios de operación y mantenimiento que debe desarrollar el prestador de servicios, incluyendo, normalmente, un reparto de responsabilidades en el que se establece a quién corresponde contratar servicios con terceros, si son necesarios. Ya hemos estudiado la importancia que tiene la adecuación del servicio a la normativa de protección de datos personales, de ahí que sea en este documento donde se plasmen las medidas de seguridad a adoptar para un correcto cumplimiento.

Dentro de los anexos debe configurarse con el contrato en la nube, por el devenir esencial para la ejecución del servicio, los denominados Acuerdos de Nivel de Servicios[387]. GARCÍA DEL POYO[388] define los ANS como los documentos que recogen las obligaciones mínimas de calidad, disponibilidad y continuidad en la prestación del servicio, así como las responsabilidades por el incumplimiento de tales obligaciones. BATISTA DE CARVALHO, DE CASTRO ANDRADE, FRANKLIN DE CASTRO, FERREIRA COUTINHO y AGOULMINE[389] especifican que los SLA son contratos

---

[386] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing". *Derecho y cloud computing*, 2012, p. 186.

[387] Dentro de las recomendaciones que establece la ENISA para las distintas entidades, según el tamaño de la organización, se recoge el establecimiento de unos Acuerdos de Nivel de Servicios que determinen las cuestiones legales asociadas a la computación en la nube.
Véase: "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009, p. 93-95. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

[388] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 64.

[389] BATISTA DE CARVALHO, Carlos André; DE CASTRO ANDRADE, Rossana Maria; FRANKLIN DE CASTRO, Miguel; FERREIRA COUTINHO, Emanuel; y AGOULMINE, Nazim: "State of the art and challenges of security SLA for cloud computing", *Computers and Electrical Engineering*, 2017, January, p. 2.

legales que definen los niveles de calidad (QoS) ofrecidos por el proveedor del servicio. El componente principal de los SLA son los objetivos de nivel de servicio, que establece el nivel de servicios mínimo a alcanzar por el proveedor de servicios, debiendo incluir niveles de indicación del servicio (SLIs) que determinan el nivel de adecuación de los niveles de servicios mínimos. Un ciclo de cinco fases se repite en la administración, gestión y contratación de los anexos ANS: la definición contractual, normalmente basado en plantillas expuestas por los proveedores del servicio; la publicación por los proveedores de esos ANS[390] y la tarea de comparación de las ofertas por parte de los clientes; la fase de negociación, una vez seleccionado un candidato adecuado a ejecutar el servicio, las partes deben acordar los términos finalmente aplicables, sobre todo los QoS y SLI; la etapa operacional, donde el monitoreo del servicio, la comparación con los adecuados niveles de servicios a través de los SLIs y los reportes de la actividad son las tareas esenciales; y, por último, la fase de finalización del servicio o desmantelamiento.

Por lo tanto, los anexos, análisis y estudio, son esenciales para una correcta materialización de la prestación del servicio, por lo que se aconseja que en el contrato marco se recojan mecanismos procedimentales para renovar estos aspectos técnicos durante la vigencia del contrato sin necesidad de modificar el acuerdo marco, dada la evolución y el progreso de esta tecnología. Los anexos configuran las especificaciones del sistema a contratar, las especificaciones de los programas a desarrollar (dependerá del servicio del *cloud*), las pruebas de aceptación, el resultado a obtener con el servicio y el análisis del objeto del contrato.

DÁVARA RODRÍGUEZ[391] recuerda que *"la formación de la voluntad y las responsabilidades de cada una de las partes, tienen una relación con la identificación personal y profesional de las mismas, que la convierten en dato de gran importancia en este tipo de contratos"*. Por lo tanto, y como se ha dejado de manifiesto a lo largo del presente trabajo, resulta de especial relevancia la identificación y situación profesional de

[390] Aunque posteriormente se utilizaran para analizar su clausulado, los proveedores suelen publicar sus ANS en sus webs corporativas. Sirva de ejemplo Google Cloud Storage SLA (https://cloud.google.com/storage/sla), Amazon EC2 Service Level Agreement (https://aws.amazon.com/es/ec2/sla/) o Microsoft Azure SLA (https://azure.microsoft.com/es-es/support/legal/sla/). Últimos accesos: 08.08.2018.

[391] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 285.

las partes que intervienen en la conformación, desarrollo y finalización del contrato de la computación en la nube[392].

a. Condiciones generales en el contrato del cloud computing.

En la contratación de los servicios del *cloud computing*, es común que los proveedores ofrezcan sus servicios a pequeñas o medianas empresas a través de portales web, lo que provoca que se acepten las "condiciones generales" mediante *clicks*, sin posibilidad de negociar término alguno, existiendo como único paso adicional la incorporación de un número de cuenta o tarjeta de crédito asociada para establecer el cargo. Como señalan ALI, KHAN y VASILAKOS[393], los servicios y recursos en la nube se realizan a través de los servicios web y de interfaces de gestión, limitando las posibilidades de interacción. Otros proveedores añaden la posibilidad de que sean los clientes quienes configuren los servicios requeridos, si bien mantienen de forma genérica los términos del contrato[394]. Este *"click-throuhg"*, influencia directa de los modelos de distribución de consumo, tiene como consecuencia que muchos usuarios no conozcan los términos del contrato establecido, es decir, no sean conscientes de la naturaleza o los efectos de las cláusulas contractuales, dado que el deseo del cliente es empezar a utilizar el servicio rápidamente, máximo cuando para utilizar ciertos productos, *wearable* o *software* requieren o incitan la contratación de la nube[395]. Es más, como han recalcado

[392] A tales efectos se recomienda leer el apartado *"Precontractual information and their impact on service level agreements"* del trabajo de DLA PIPER UK LLP - COMISIÓN EUROPEA: "Comparative study on cloud computing contracts", 2015, p. 32-34. Accesible en: http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/. Último acceso: 08.08.2018. Se realiza un estudio del Derecho comparado sobre la vinculación legal de la información precontractual en los Acuerdos de Niveles de Servicio y la obligatoriedad del proveedor de servicios de proporcionar la información relevante a la contraparte, con independencia incluso de que sea considerado consumidor o usuario.

[393] ALI, Mazhar; KHAN, Samee U.; y VASILAKOS, Athanasios V.: "Security in cloud computing: Opportunities and challenges", *Information Sciences*, 2015, 305, p. 359.

[394] Para la contratación del *cloud* público de ADW.ES puedes elegir el almacenamiento, el procesador disponible, la memoria garantizada para el servicio, el disco duro HA, las direcciones IP disponibles, el sistema operativo, la posibilidad o no de panel de control, posibilidades de administración y otros servicios avanzados. Más información accesible en: https://www.adw.es/servidores-cloud.html. Último acceso: 08.08.2018.

[395] Sirva de ejemplo que para poder usar móviles Apple se requiere estar suscrito a una cuenta iCloud, y como los productos móviles con sistema operativo Android sugieren, en los primeros pasos, tener una cuenta con Google, además de la propia del fabricante del *hardware***,** por ejemplo, Samsung Cloud.

HON, MILLARD y WALDEN[396], el utilizar servicios en nube gratuitos o *low cost* no implica, necesariamente, estar libre de riesgos asociados, dado que no seguir un procedimiento de contratación empresarial ocasiona riesgos legales, reglamentarios o de reputación, más si cabe cuando se utilizan datos reales, confidenciales y personales.

Por lo tanto, los usuarios de los servicios en nube deben ser diligentes a la hora de utilizar el servicio, llevando a cabo un estudio de las cláusulas que regirán la prestación del servicio en una fase pre-contractual, no solo cuando se realice una migración completa o se procesen datos reales, con más sigilo si procesan datos personales, sino en cualquier estadio inicial o de prueba que requiera procesos en la nube. Por este motivo, parece oportuno realizar un análisis detallado de las cláusulas tipo que nos podemos encontrar en un contrato de *cloud computing*.

i. Contratantes, parte expositiva y el objeto del contrato

La identificación de las partes intervinientes en el contrato es de gran importancia, debiendo determinarse no solo quién adquiere la responsabilidad de la contratación y a quién representa, supuesto de una contratación entre empresarios, sino qué conocimientos o formación relacionada con el objeto del contrato tiene cada una[397]. De este modo, la formación de la voluntad y las responsabilidades de las partes tienen una relación directa con la identificación de los contratantes y su formación en el sector.

A continuación, se recogerá la parte expositiva. En ella se enumeran con detalle las necesidades por las que se requiere el servicio del *cloud*, que recaen en el cliente, y las posibilidades de prestar el servicio requerido adecuado a las necesidades del usuario, expositivos que recaen en el proveedor de servicios en nube[398]. Estos expositivos deben formularse de forma clara y concreta, determinando el porqué y para qué del contrato, atendiendo a las necesidades, condicionantes e intenciones por la cual las partes celebran y formalizan el contrato de computación en la nube. Debe existir coincidencia real, entre

[396] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 6.

[397] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 285-286.

[398] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing". *Derecho y cloud computing*, 2012, p. 188.

las partes, sobre el objeto del contrato. Como puede aventurarse, muchos contratos estandarizados adolecen de este cuerpo expositivo.

De gran utilidad es lo manifestado por DÁVARA RODRIGUEZ[399]:

"*es de interés establecer claramente el negocio jurídico en el cual luego, de acuerdo con la teoría general para ese negocio en el ordenamiento, se pueda subsumir el caso e interpretar el contrato".*

Por último, de entre las cláusulas que condicionan el contrato de *cloud computing* destaca el objeto del contrato, dado que determinará la interpretación del contrato y las cláusulas específicas, estructurando y conformando las condiciones que se han contratado. Delimitar el objeto del contrato reestablecerá el desequilibrio inicial y la posición dominante que adolece el *cloud*, que como hemos indicado ostenta el proveedor de servicios.

Este modelo lo sigue el servicio CLOUDBUILDER NEXT de ARSYS[400].

En la parte expositiva se delimita de forma clara la personalidad jurídica de la entidad que desarrollará el servicio, incluyendo, entre otros, el notario ante el que está constituida la sociedad y la inscripción en el Registro Mercantil oportuno. Sin embargo, y como claro ejemplo del *click-throuhg,* para el cliente se establece *"de otra parte el contratante, persona física o jurídica que cumplimenta el formulario de contratación (en adelante el Cliente), que aparece en https://shop.arsys.es/, con los datos exigidos y con el que arsys establece una actividad comercial a través de estas Condiciones Específicas. El contratante conoce, entiende y acepta libremente, tras informarse de las características de cada servicio, las presentes Condiciones"*. Con esta fórmula podemos aventurar claramente el desequilibrio de las partes en el contrato, no tanto porque no se establezca la posibilidad de ampliar la identidad del contratante a través de cláusulas abiertas, sino que directamente para contratar exige que la parte "conozca, entienda y acepte *libremente, tras informarse de las características de cada servicio, las presentes Condiciones*".

---

[399] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 286.

[400] Se puede acceder a las condiciones de CLOUDBUILDER NEXT de ARSYS a través del siguiente enlace: https://www.arsys.es/legal?dhtml=contrato-ngcs. Condiciones a fecha de 08.08.2018 (Ref.: CECBN_141217). Último acceso: 08.08.2018.

No se limita aquí las deficiencias en el contrato. Aunque recoja la definición de diversos términos contractuales, en su mayoría de naturaleza informática, remite *"el contenido comercial, la información sobre recursos, características y precios de la plataforma"* a la información que, de forma frecuente, se irá actualizando en la web principal. Aunque posibilita que los términos del contrato no sufran grandes variaciones con las innovaciones tecnológicas, limita la capacidad de un entendimiento completo del cliente, recayendo en este último una tarea continua de investigación y revisión.

Sí tiene un alcance completo el objeto del contrato a través de dos cláusulas, la definida como "objeto" y la establecida como "características de la plataforma de CLOUDBUILDER NEXT".

A pesar de las indicadas deficiencias del servicio de ARSYS, más acuciadas son las presentes en el servicio de computación en la nube de VIRTUAL DATA CENTER (VDC) de CLARANET[401].

En la descripción del objeto recoge simplemente que "*el Servicio de Virtual Data Center, en adelante VDC, proporcionado por CLARANET permitirá al CLIENTE dar de alta y gestionar sus propios Servidores virtuales, y alojar en ellos información y contenidos a través de un portal web (Portal Cloud) puesto a disposición del CLIENTE. Dicho servicio funciona sobre la plataforma VDC de CLARANET y se configura de acuerdo a los recursos, capacidad de almacenamiento y demás especificaciones técnicas acordadas con el CLIENTE a través del Formulario de Contratación"*. Es tal la limitación en la fase pre-contractual a la que se enfrenta el cliente, que antes de contratar con CLARANET no tiene posibilidad ni de evaluar de forma clara el servicio que va a contratar, se limita a establecer una definición, ni de analizar el denominado "Formulario de Contratación", solo accesible bajo un *check-box* en la última fase de la compra telemática del servicio. Sí recoge parámetros de monitorización y disponibilidad que serán analizados posteriormente.

Para identificar la personalidad jurídica del proveedor debemos acceder a las "Condiciones Generales de los servicios de Claranet, S.A.U.", documento disponible para todos los servicios de la entidad, diferenciado del principal regulador del servicio.

[401] Las condiciones del servicio de VIRTUAL DATA CENTER (VDC) de CLARANET pueden estudiarse en: https://www.claranet.es/legal/condiciones-particulares-de-los-servicios-de-vdc. Para nuestro estudio se ha utilizado la última actualización hasta la fecha, de octubre de 2016. Último acceso: 08.08.2018.

De esta breve inmersión en diferentes servicios de *cloud* que ofertan las empresas puede avistarse las dificultades con las que se encuentran los clientes que contratan la nube. El conflicto por identificar el proveedor del servicio, la problemática en la correcta definición del servicio a contratar y los inconvenientes para analizar, ante el ocultismo de la información, las cláusulas que determinarán el contenido del contrato, son aspectos presentes en la contratación ante clientes de pequeña o mediana entidad. Salvo personas jurídicas con un gran poder negociador, el marco teórico y el ejemplo práctico serán difícilmente reconciliables.

ii. Obligaciones de las partes

En los contratos informáticos, como el que ahora estudiamos, la necesidad de que los compromisos que adquieran las partes se recojan de forma clara cobra vital importancia. La cláusula, que puede subdividirse en las obligaciones que conciernen a cada parte, deviene fundamental para la formalización del contrato. En este sentido, se deben identificar los elementos que guardan relación con las obligaciones asumidas por cada parte, de otro modo podría devenir responsabilidad por falta de adjudicación de las obligaciones[402].

El cliente de la nube tiene, como obligación principal, el pago del precio por los servicios ofrecidos. Por lo tanto, el contrato deberá establecer los precios fijos a los que debe someterse el cliente y los pagos en función de los servicios o productos adicionales. Si el contrato no tiene contraprestación dineraria, los llamados "gratuitos", será esencial determinar la contraprestación del cliente, que principalmente será a cambio de la cesión de datos o de derechos relacionados con la propiedad intelectual. En cuanto al precio, el artículo 10.1.f de la LSSICE requiere que la información se proporcione de manera clara y exacta, indicando si incluyen o no los impuestos aplicables[403]. A esta obligación principal, se debe añadir el cumplimento de las políticas de uso adecuado y el deber de colaboración con el proveedor de servicios, deber estrechamente vinculado al principio de buena fe contractual. En caso de incumplimiento, devendrá la responsabilidad del cliente.

---

[402] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing". *Derecho y cloud computing*, 2012, p. 189.

[403] Esta información puede aparecer recogida en la web del proveedor, siempre que sea permanente, de fácil acceso, directa y gratuita, artículo 10.2 de la LSSICE.

El prestador del servicio tiene que garantizar la disponibilidad, la integridad y la confidencialidad de los datos, y el desarrollo de una política de seguridad acorde con el servicio. Estas obligaciones se relacionan con las características propias del *cloud*, configurado como una herramienta de acceso a través de Internet, un servicio bajo demanda, que requiere elasticidad y rapidez en la provisión, y mensurable, por lo que es necesario convenir las condiciones de continuidad, regularidad, velocidad, volumen y seguridad. El proveedor se obliga, por tanto, al acceso ininterrumpido del cliente a los recursos, con una calidad determinada (manteniendo las características anteriormente reseñadas), y a colaborar y facilitar al cliente la información relativa al producto, así como sus características esenciales (por ejemplo, la política de seguridad) para facilitar la correcta elección conforme sus necesidades.

En el establecimiento de la cláusula que regula las obligaciones de las partes debe buscarse la sistematización y la claridad de redacción, con el fin de evitar conflictos en la interpretación o exigencias de responsabilidad por incumplimiento de las obligaciones. Es en esta cláusula, junto con la que determina el objeto del contrato, donde se establecen las premisas que determinarán el modelo de computación en la nube contratado, dentro de los tipos de servicios existentes. De este modo, el beneficiario de los servicios podrá contrastar que los productos que contrata se asemejan a las necesidades requeridas, necesidades que tienen reflejo en las obligaciones que tiene que asumir el prestador de servicios. Sin embargo, cada vez son más los proveedores que establecen una cláusula genérica para todos los servicios informáticos que ofrecen, detallando las concretas obligaciones en anexos posteriores[404]. Por consiguiente, esta cláusula debe correlacionarse con los ANS, que deben delimitar de manera precisa las obligaciones de resultado para el proveedor de servicios de computación en la nube. En consecuencia, la cláusula que determina las obligaciones de las partes puede tener un contenido más genérico, tener un alcance más general.

Para los servicios de MOVISTAR CLOUD[405], el proveedor establece un acuerdo concreto de obligaciones para las partes en los servicios de la nube. Se divide en las cláusulas 7 y 8, entre las obligaciones del cliente y del usuario y del proveedor del

[404] Sirva de ejemplo CLARANET, estudiado anteriormente.

[405] Las condiciones del servicio de MOVISTAR CLOUD pueden estudiarse en: http://www.movistar.es/rpmm/estaticos/residencial/fijo/servicios-sobre-adsl/contratos/condiciones-servicio-movistar-cloud.pdf. No indica la fecha de actualización o versión de las condiciones. Último acceso: 08.08.2018.

servicio. Como se ha expuesto *ad supra*, del estudio de las cláusulas puede aventurarse que para un conocimiento exacto debamos acudir a anexos adicionales. De forma genérica se establece un manifiesto sobre el correcto uso de los servicios y de la responsabilidad por daños y perjuicios padecidos por las partes. Si bien, hay cláusulas que determinarán el contenido posterior del contrato. En primer lugar, para los clientes y usuarios, con incidencia directa en las posteriores cláusulas sobre la protección de la propiedad intelectual e industrial, aparece una exención de responsabilidad del proveedor por los usos del cliente, incorporando instrucciones para un correcto uso del servicio. Indica que *"Movistar no será responsable de las infracciones de cualquier Cliente o Usuario que afecten a los derechos de terceros, incluyendo los derechos de copyright, marcas, patentes, información confidencial y cualquier otro derecho de propiedad intelectual o industria"*, añadiendo que *"el Cliente y, en su caso, los Usuarios serán los únicos y exclusivos responsables de los daños que pudieran ocasionarse por incumplimiento de la legislación vigente o de las obligaciones asumidas en virtud de las presentes Condiciones. El Cliente protegerá y mantendrá indemne a Movistar contra toda reclamación judicial o extrajudicial que tuviera relación con incumplimientos por su parte o por parte de los Usuarios, así como con cualquier gasto, daño, carga u obligación con causa en dichos incumplimientos"*.

En otro orden, en las obligaciones referentes al proveedor, resulta relevante cómo, a pesar de comprometerse a instalar los medios técnicos exigibles para garantizar el secreto de las comunicaciones, sobre todo en tránsito, queda *"exonerada de cualquier responsabilidad que pueda derivarse de la obtención por parte de terceros de Contenidos almacenados en el Servicio Movistar Cloud o del daño que terceros puedan provocar en los mismos"*, además del funcionamiento anormal por tareas de mantenimiento, de las intercepciones legales del servicio e incluso establece la posibilidad de limitar el servicio, entre otros, por la sospecha de almacenamiento ilegal o peligroso o carga excesiva del sistema.

Por lo tanto, claramente se vislumbran las grandes deficiencias que a lo largo del trabajo hemos expuesto con los denominados contratos informáticos de adhesión, la exoneración de responsabilidad por parte del proveedor de servicios en acciones o usos que claramente radican en sus actividades para ofrecer el servicio. Habrá que atender a los ANS para su determinación.

Una mejora importante se recoge en las obligaciones del proveedor VELNEO[406] para sus servicios de *cloud*. A pesar de reservarse la posibilidad de interrumpir el servicio por tareas de mantenimiento y reparación se establece ya, en las condiciones generales, que *"lo notificará con la antelación suficiente en función de las circunstancias de cada caso mediante correo electrónico a la cuenta de correo de contacto que figure. Las paradas por mantenimiento y mejora de los servicios programadas se comunicarán al menos con 72 horas de antelación"*. Permite la planificación de los clientes y usuarios ante la parada del servicio. Aunque Internet tenga ámbito global, puede favorecer la adopción del servicio por el cliente el hecho de que las condiciones de uso sean comprensibles para los usuarios. VELNEO se compromete a que *"los contratos de sus productos, el procedimiento de contratación y la información publicada en su página web exclusivamente en idioma castellano"*.

A pesar de estas mejoras, las políticas de VELNEO hacen recaer en el cliente la total decisión de la contratación de unos servicios que, por su complejidad y tecnificación, puede no estar preparado para su correcta elección. Se pretende resolver la desigual capacitación de las partes, a las que hacíamos referencia al inicio del capítulo, con la expresa manifestación de que "*El CLIENTE reconoce haber decidido que configuración de la plataforma VELNEO CLOUD se adecúa mejor a sus necesidades y que ha sido informado por parte de VELNEO adecuadamente, garantizando el CLIENTE que utilizará los recursos disponibles de acuerdo con las especificaciones y restricciones técnicas facilitadas por VELNEO"*. La posibilidad de que sea asesorado por el proveedor para la correcta elección del servicio es difusa, por cuanto el soporte comercial se limita a una enumeración de las características del servicio ofrecido, recayendo en el cliente la necesidad de un conocimiento exacto de los requerimientos físicos y logísticos (*hardware* y *software*) que posee, cómo incidirán los niveles de servicio ofrecidos en las necesidades requeridas y cómo extrapolar la información recibida por el proveedor en el abanico de ofertas de otros proveedores, entre otros.

iii. Protección de datos de carácter personal

En el Capítulo IV, sobre todo en el apartado .b, hemos realizado un extenso estudio sobre la relevancia de preservar los datos personales en el entorno del *cloud computing* y

[406] Las condiciones del servicio de VELNEO CLOUD pueden estudiarse en: https://velneo.es/politicas/cloud/. El acuerdo revisado es el último hasta la fecha, de enero de 2013. Último acceso: 08.08.2018.

las incidencias en el desarrollo de la prestación del servicio a la luz de la normativa aplicable, remitiéndonos a las conclusiones allí expuestas.

En síntesis, sería importante que se recogiera en el clausulado del contrato, como mínimo, si estamos en un supuesto de comunicación de datos a terceros o se está realizando un encargo de tratamiento de datos personales; quién es el responsable del fichero de datos, aunque se deduzca de la normativa y del servicio contratado; si el proveedor actúa como encargado del tratamiento; las medidas de seguridad que se adoptarán a tenor de los datos tratados, incluso de los datos en tránsito; y la exclusión o posibilidad de realizar cualquier subencargo del tratamiento, al incidir de manera particular el establecimiento del tercer agente en la exigencia de una protección jurídica adecuada.

ARSYS en la contratación de CLOUDBUILDER NEXT[407] establece, en su cláusula décima, la política de protección de datos de carácter personal aplicable. A pesar de reconocer que los proveedores técnicos de algunos productos pueden acceder de forma remota al servidor físico, lo que viene a suponer una subcontratación en alguno de los servicios sin especificar cuáles, recoge que solo se limitaría *"a la ejecución de los trabajos necesarios para resolver la incidencia, sin utilizar la intervención ni los datos a los que pudieran tener acceso para otros fines"*. Por lo tanto, intenta garantizar que no se realiza ningún tratamiento de datos.

Sin embargo, creemos que lo más relevante es la información relativa a la ubicación del centro de datos cuando se contrata el servicio bajo servidores en Estados Unidos. ARSYS señala la ciudad, el estado y la propiedad a la que pertenece, y con la que subcontrata, los servicios de alojamiento cuando se realiza esta opción. Esta cláusula que favorece la trasparencia para la toma de decisiones del cliente, por cuanto conocerá el domicilio y dónde, lugar, se alojan sus datos y la previsible normativa aplicable, está correlacionada con dos aspectos fundamentales: la delimitación de las medidas y normativa aplicable, que en su lugar el proveedor ahora señala *"que siendo tratada por la entidad antes mencionada, con un nivel de protección distinto al establecido en la normativa española de protección de datos"*; y la asunción por el cliente de la posición de responsable del tratamiento, que aunque no lo especifique en el clausulado, le impone,

[407] Se puede acceder a las condiciones de CLOUDBUILDER NEXT de ARSYS a través del siguiente enlace: https://www.arsys.es/legal?dhtml=contrato-ngcs. Condiciones a fecha de 08.08.2018 (Ref.: CECBN_141217). Último acceso: 08.08.2018.

esto sí de forma expresa, el deber de *"informar de dicha circunstancia a los titulares de los datos que pudieran verse afectados por dicha transferencia y tratamiento, así como obtener la autorización de los mismos en aquellos casos en que fuera necesario"*. Advierte, además, de la posibilidad de recabar datos, a través del proveedor, de la autoridad competente en el lugar del alojamiento.

Por lo expuesto, puede apreciarse que no se recoge de manera clara un cuerpo que regule la protección de los datos personales cuando se contratan los servicios de la nube. Ahondando un poco más, ya en los denominados "avisos legales"[408], genérico para todos los servicios informáticos de ARSYS, sí se recoge información de vital importancia para calibrar la actuación del proveedor en el desarrollo del servicio. En la cláusula 10.9 reseña la calificación del proveedor de servicios, de conformidad con el artículo 28 del RGPD y el artículo 12 de la LOPD y su reglamento de desarrollo: *"arsys actuará como encargado del tratamiento"*. Si bien, para el acceso y/o tratamiento establece los requisitos, expuestos como prerrequisitos para ser considerado responsable, del tratamiento conforme a las instrucciones del cliente y bajo los fines contractuales. Aclara y reconoce que cuando ARSYS destine los datos a otra finalidad, será considerado responsable del tratamiento.

Es en este documento genérico donde el proveedor establece la política de subcontratación del servicio, que, al ser aceptado por el cliente, lo autoriza a subcontratar con terceros. Aunque permite al cliente dirigirse al proveedor del servicio para recabar información de los subproveedores, no se recoge, a priori, ningún listado o cuadro de posibles terceros a los que subcontratar el servicio, así como la localización de los centros de datos de esos subproveedores. Por lo tanto, la aceptación de los términos legales indicados supone un cheque en blanco para el proveedor de la nube, pudiendo subcontratar los servicios con proveedores con niveles de protección más laxos.

Por último, relacionado directamente con las facultades de recuperación de datos e información del cliente, analizadas en subapartados sucesores, hay que recordar que el RGPD establece la potestad al interesado de solicitar del responsable del tratamiento la portabilidad de los datos personales transferidos a la nube, debiendo informar,

[408] Se puede acceder a las CONDICIONES GENERALES DE SERVICIO de ARSYS a través del siguiente enlace: https://www.arsys.es/legal?dhtml=condiciones-generales-contratacion. Condiciones a fecha de 08.08.2018 (Ref.: CGS_230518). Último acceso: 08.08.2018.

igualmente, sobre el plazo de conservación de los datos personales y el plazo durante el cual se conservarán los datos[409]. Nada aparece, en los contratos analizados, sobre esta nueva obligación del responsable del tratamiento, que necesariamente requiere la colaboración del proveedor de la nube.

iv. Duración y terminación del contrato

Uno de los aspectos esenciales en la contratación del servicio en nube, y que debe ser tratado antes de la formalización del contrato, es el plazo mínimo y máximo aceptable del contrato para las partes, así como la estrategia de salida a emplear, dado que un contrato con una duración elevada puede ser una fuerte barrera, *lock-in*, en la implantación del servicio[410].

Un plazo mínimo inicial, impuesto por el proveedor del servicio, puede estar justificado ante grandes demandas de servicios, que requieran una oferta sofisticada y personalizada para el cliente. Solo ante un servicio especialmente personalizado puede considerarse equilibrado, por los costes asociados que tiene el proveedor, así como una penalización por cancelación anticipada y que obliga, por tanto, establecer una duración mínima. Por consiguiente, el establecimiento de unos compromisos de permanencia, dependiente en gran manera de los servicios requeridos, tiene como justificación la inversión que el proveedor del *cloud* puede requerir por la dependencia de unos servidores que ofrezcan la capacidad técnica contratada.

El servicio de BACKUP EN LA NUBE[411] de QUERRY S.A. establece una duración mínima del contrato de un año, renovado tácitamente por un nuevo año a la expiración de cada período anual. Sin embargo, en servicios más estandarizados el período de duración

---

[409] El considerando 39 del RGPD establece que *"para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica"*. Concretándose, entre otros, en el artículo 5.1.e: *"*(los datos personales serán) *mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales"*.

[410] HON, W. Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 34.

[411] Se puede acceder a las CONDICIONES DEL SERVICIO DE BACKUP EN LA NUBE de QUERRY S.A. a través del siguiente enlace: http://www.querry.com/wp-content/uploads/2015/07/cgbn100516.pdf. Condiciones a fecha de 08.08.2018 (REF.: jmm100516bn). Último acceso: 08.08.2018.

se adapta de forma elástica. TVP en LA NUBE[412] establece una duración mínima de 30 días desde la firma del pedido.

Igualmente pueden recogerse causas de terminación anticipada del contrato, principalmente relacionadas con la insolvencia y la violación grave de los términos del contrato[413]. Por el fraudulento uso de las nuevas tecnologías, se ha añadido como causa común de la terminación del contrato la recepción de denuncias de terceros por incumplimientos de derechos de propiedad intelectual o industrial. En este marco, parece oportuno recoger por parte de los clientes un preaviso antes de la terminación efectiva del servicio, así como, en la medida en que fuera posible e identificable (especialmente ante las infracciones relacionadas con la propiedad intelectual), que la suspensión o terminación se localice en ese servicio concreto, no en la totalidad del *cloud*, para lo cual la colaboración del usuario se hace necesaria. Tenemos constancia de que algunos proveedores establecen un plazo desde la notificación, antes de la terminación del servicio, para que los clientes puedan subsanar el incumplimiento, medida muy favorable para el usuario en el desarrollo del servicio[414].

AMAZON para los servicios de AWS[415], en la cláusula 7.2.A, reconoce que *"we may terminate this Agreement for any reason by providing you at least 30 days' advance notice"*. Sin embargo, ARSYS en las CONDICIONES GENERALES DE SERVICIO[416] elimina cualquier tipo de aviso previo de resolución: *"si el incumplimiento del cliente fuera causa de resolución de estas CGS,…, se reserva el derecho a terminar de forma anticipada la relación contractual y, por lo tanto, a desposeer al cliente de los productos*

[412] Se puede acceder a las CONDICIONES GENERALES DE CONTRATACIÓN de TPV EN LA NUBE a través del siguiente enlace: http://tpvenlanube.com/images/contratos/ContratoClienteTPV.pdf. Condiciones a fecha de 08.08.2018. Último acceso: 08.08.2018.

[413] Debe tenerse en cuenta que la mayoría de los proveedores de servicios de *cloud* establecen sus condiciones generales, al igual que *acceptable use policy* (AUP), como términos estandarizados (lo "tomas o lo dejas").

[414] En el Capítulo V.a.c se realiza un estudio sobre la extinción del contrato de *cloud*, sus causas y sus efectos en las obligaciones.

[415] Se puede acceder al CUSTOMER AGREEMENT de AWS a través del siguiente enlace: https://aws.amazon.com/es/agreement/. Condiciones a fecha de 08.08.2018 (Última modificación: 01.07.2018). Último acceso: 08.08.2018.

[416] Se puede acceder a las CONDICIONES GENERALES DE SERVICIO de ARSYS a través del siguiente enlace: https://www.arsys.es/legal?dhtml=condiciones-generales-contratacion. Condiciones a fecha de 08.08.2018 (CGS_23052018). Último acceso: 08.08.2018.

o servicios contratados sin previo aviso y sin derecho a reclamar indemnización o devolución de cantidad alguna".

En AWS se reconoce la posibilidad de subsanar el incumplimiento, de cualquiera de las partes, de los términos pactados, estableciendo un plazo desde la notificación: "*either party may terminate this Agreement for cause if the other party is in material breach of this Agreement and the material breach remains uncured for a period of 30 days from receipt of notice by the other party. No later than the Termination Date, you will close your account"*. No solo por el plazo para la subsanación del incumplimiento esta cláusula supone un equilibrio entre las partes, sino porque la opción se declara para ambas partes, cliente y proveedor, no siendo común ante cláusulas de adhesión otorgar dicha capacidad al cliente.

Una medida intermedia, y preventiva, es la suspensión del servicio. Permite al cliente y al proveedor argumentar las actuaciones que presuponen la vulneración de los acuerdos establecidos para el servicio, y en último término faculta al cliente para la subsanación de los incidentes que el proveedor considere causa de su incumplimiento[417]. La mayoría de los proveedores de *cloud* que han establecido causas de suspensión las vinculan a un comportamiento directo del cliente, como falta de pago o incumplimiento de las condiciones generales (o de las AUP). Incluso en algunos supuestos, se ha establecido la suspensión del contrato por razones ajenas a los usuarios (clientes), por ejemplo, tras un incidente de seguridad o para hacer frente a los problemas del servicio técnico.

TVP en LA NUBE en sus CONDICIONES GENERALES DE CONTRATACIÓN[418] establece que *"transcurridos un máximo de 48 horas desde el aviso, sin que se ejecute el pago de los importes pendientes, WCB podrá suspender el servicio contratado"*. Sin embargo, y aunque posteriormente se estudiarán las cláusulas referentes a la responsabilidad, el proveedor indica expresamente que *"no se responsabiliza de las consecuencias que pudieran resultar como consecuencia de la desactivación o suspensión…"*, si bien, reconoce que ante una suspensión del servicio en

[417] HON, W. Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 37.

[418] Se puede acceder a las CONDICIONES GENERALES DE CONTRATACIÓN de TPV EN LA NUBE a través del siguiente enlace: http://tpvenlanube.com/images/contratos/ContratoClienteTPV.pdf. Condiciones a fecha de 08.08.2018. Último acceso: 08.08.2018.

la cual el cliente no haya violado ninguna de las condiciones establecidas para la contratación, se le restituirá al cliente los importes no consumidos. No incluye, a tenor de la anterior cláusula, las indemnizaciones por los daños y perjuicios causados ante la suspensión de la nube, por ejemplo, la no disponibilidad de la web corporativa de ventas.

En el BUSINESS AGREEMENT[419] de DROPBOX (cláusula 4.2) se recoge la posibilidad de suspender la prestación del servicio si se produce una "emergencia de seguridad"[420].

Consecuencia de la terminación del contrato de la nube es el régimen de devolución de los datos almacenados, circunstancia que genera gran debate en torno a la obligatoriedad o no del proveedor del servicio de llevar a cabo la acción. Aunque su estudio se pospone al apartado de las cláusulas específicas del contrato, sirva de introducción que, pudiendo las partes acordar lo que estimen oportuno, en términos generales el cliente no tiene derecho, con la salvedad expuesta en términos de protección de datos personales, de reclamar la recuperación de los datos trasladados a la nube. Sin embargo, dada la importancia del problema planteado, en el Derecho comparado se han desarrollado teorías jurídicas para reafirmar el derecho de recuperación de datos, teniendo como base el principio de la buena fe contractual y el marco regulatorio de los contratos de arrendamientos[421].

v. Jurisdicción y ley aplicable

Cuando las partes son empresas o empresarios se suele pactar la jurisdicción y la ley aplicable, si bien, suele imponerse de forma reiterada la relacionada con el

[419] Se puede acceder DROPBOX BUSINESS AGREEMENT a través del siguiente enlace: https://www.dropbox.com/terms#business_agreement.. Fecha de publicación: 17.04.2018. Último acceso: 08.08.2018.

[420] De forma literal, utilizando la versión en inglés al prevalecer en caso de discrepancias con otros idiomas, *"notwithstanding anything in this Agreement, if there is a Security Emergency then Dropbox may automatically suspend use of the Services. Dropbox will make commercially reasonable efforts to narrowly tailor the suspension as needed to prevent or terminate the Security Emergency"*.

[421] DLA PIPER UK LLP - COMISIÓN EUROPEA: "Comparative study on cloud computing contracts", 2015, p.10 y p. 51-53. Accesible en: http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/. Último acceso: 08.08.2018.

establecimiento principal de negocios del proveedor de servicios[422]. En el *cloud*, la renuncia expresa al fuero que pudiera corresponder en función del contenido del contrato cobra relevancia, más cuando los principales suministradores del servicio se rigen por el *common law*.

Recuerda MERCHÁN MURILLO[423], que el Convenio de la Haya sobre Acuerdos de Elección del Foro[424], hecho el 30 de junio de 2005, permite a las partes en operaciones comerciales, entre las que puede considerarse la contratación de la computación en nube entre empresarios o profesionales, elegir el juez al que someterse, de forma exclusiva, en los litigios que pudieran surgir en el desarrollo de la relación contractual. Su aplicabilidad está condicionada a la concurrencia de tres requisitos o condicionantes: la internacionalización de la situación, el carácter civil o comercial de la controversia y la existencia de un acuerdo exclusivo de elección del foro.

Esta práctica se ha extendido fuera de las empresas angloamericanas. ARSYS, entidad con domicilio social en Logroño (La Rioja), recoge en sus CONDICIONES GENERALES DEL SERVICIO[425], la renuncia del fuero propio, de ser otro, a favor de la jurisdicción y competencia de los Juzgados y Tribunales de Logroño. Sin embargo, claramente hay una diferencia con la cláusula estipulada al efecto para los servicios en HOSTALIA[426]. Mientras en ARSYS se destaca que esa renuncia al foro es *"en los casos que las normas procesales lo permitan"*, HOSTALIA utiliza una terminología más impositiva, *"con renuncia expresa a cualquier otro fuero que en derecho pudiera*

---

[422] BRADSHAW, Simon; MILLARD, Christopher y WALDEN, Ian: "Contracts for Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", *Queen Mary University of London - Legal Studies Research Paper,* 2010, nº 63, p. 18.

[423] MERCHÁN MURILLO, Antonio: "Cloud computing: soluciones ante un posible conflicto de leyes", *Revista La Ley Mercantil,* 2018, nº48, junio 2018. Acceso a través del servicio digital La Ley Digital (bajo suscripción).

[424] Accesible en: https://assets.hcch.net/docs/4ddb0a2b-327d-47c3-89f1-bc15679ffc99.pdf. Último acceso: 08.08.2018.

[425] Se puede acceder a las CONDICIONES GENERALES DE SERVICIO de ARSYS a través del siguiente enlace: https://www.arsys.es/legal?dhtml=condiciones-generales-contratacion. Condiciones a fecha de 08.08.2018 (Ref.: CGS_23052018). Último acceso: 08.08.2018.

[426] Accesible los TÉRMINOS Y CONDICIONES DEL CONTRATO de HOSTALIA en: https://www.hostalia.com/contratar/contrato.html. Condiciones a fecha de 08.08.2018. Último acceso: 08.08.2018.

corresponderles"[427]. Aunque a efectos prácticos el resultado es idéntico, porque prevalecerá en todo caso lo que es justo a derecho cuando las normas no tengan carácter dispositivo, el lenguaje draconiano posiblemente dificultará un entendimiento posterior entre las partes.

Un problema adicional es el establecimiento de cláusulas contractuales que establecen, para poder ejercer una reclamación por los servicios prestados, unos plazos de prescripción excesivamente cortos. ADRIVE en los TERMS OF SERVICE[428], cláusula 23 ("*Time Limitation on Claims*") que precede a la que regula el derecho aplicable y el arbitraje (cláusula 24, "*Governing Law & Arbitration*"), limita la posibilidad de cualquier reclamación a un plazo máximo de 6 meses desde que el cliente tuvo o pudo tener constancia de las causas que dan lugar a la controversia[429]. APPLE para IWORK.COM[430] establece que la reclamación podrá presentarse, como máximo, un año después de producirse la causa de la reclamación o demanda[431].

La renuncia al foro suele ir ligada a una asunción del arbitraje como medio idóneo para dirimir los conflictos o diferencias que pudieran surgir entre las partes del contrato en la interpretación y aplicación de las condiciones contractuales. En un sector empresarial tan especializado es bastante habitual que las disputas y conflictos se

---

[427] Cláusula nula, *contra legem*, si el cliente fuere considerado consumidor. En el próximo epígrafe se estudiarán los contratos B2C.

[428] Se puede acceder a los TERMS OF SERVICES de ADRIVE en: http://www.adrive.com/terms. Condiciones a fecha de 08.08.2018 (Última actualización: 22.09.2015). Último acceso: 08.08.2018.

[429] Atendiendo a los artículos 942 y ss. del Código de comercio y los artículos 1961 y ss. del Código civil, esta regulación de la preinscripción contraviene las normas establecidas para las acciones nacidas de la responsabilidad por incumplimiento de las obligaciones del contrato, artículo 1964 del Código civil, incluso de la responsabilidad extracontractual, artículo 1902 del Código civil. El carácter imperativo de las normas reguladoras de la prescripción se justifica por favorecer la seguridad del tráfico, al aclarar y delimitar la vigencia de los derechos de las partes (REGLERO CAMPOS, Luis Fernado: "ARTS. 744-773; 1278-1280; 1961-1975", *Jurisprudencia Civil comentada*, 2000, Comares, p. 3427-3443). Para un completo estudio de la imperatividad de las normas de prescripción ver DIEZ-PICAZO Y PONCE DE LEÓN, Luis: *La Prescripción Extintiva - en el Código civil y en la jurisprudencia del Tribunal Supremo (estudios y comentarios de legislación)*, 2007, Civitas.

[430] LAS CONDICIONES DE SERVICIO de IWORK.COM son accesibles en el siguiente enlace: https://www.apple.com/legal/iworkcom/es/terms.html. Condiciones a fecha de 08.08.2018 (Última revisión de 19.01.2010). Último acceso: 08.08.2018.

[431] A modo de curiosidad, ambos servicios declaran excluida la Convención de las Naciones Unidas sobre contratos para la venta internacional de productos, aunque los objetos regulados no se pueden considerar mercaderías, estando, por tanto, fuera del ámbito de aplicación del Convenio.

resuelvan ante órganos especializados fuera del ámbito jurisdiccional, en busca de una mayor eficacia y rapidez. LÓPEZ JIMÉNEZ[432] resalta cómo en los contratos transfronterizos, como suele suceder con los contratos electrónicos, la vía de resolución de conflictos extrajudicial evita tres aspectos perjudiciales para el desarrollo de este comercio: la incompatibilidad entre la rapidez del tráfico mercantil y la lentitud del desarrollo judicial; la determinación del tribunal competente y la legislación aplicable; y la ejecución de una resolución fuera del país donde se dictó. La mediación y el arbitraje, sobre todo este último, se están imponiendo en el desarrollo de las prestaciones de servicios informáticos al concurrir, comúnmente, elementos de carácter internacional. De otra forma, un conflicto entre las partes podría prolongarse durante años y resultar extremadamente costoso. Por este hecho, acudir al sistema arbitral podría evitar el sometimiento a jurisdicciones extranjeras ajenas al conocimiento de alguna de las partes del contrato[433]. Algunas entidades recogen al arbitraje como prioritario, como ARSYS, y otras con carácter excluyente, este es el caso de ADRIVE.

En una relación entre empresarios, el criterio predominante es la libre elección de la ley aplicable por las partes, que puede resultar de la manifestación expresa de los intervinientes en el contrato, de la interpretación de los términos del contrato o de las propias circunstancias del caso[434]. El Reglamento (CE) nº 593/2008 del Parlamento europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales[435], Roma I, permite que las partes designen la ley aplicable a la totalidad del contrato o solamente a una parte, artículo 3.

b. Cláusulas específicas en el contrato del cloud computing.

La complejidad de los servicios de la nube suele imposibilitar una ordenación completa de todo el servicio, requiriendo el asesoramiento externo profesional, repetido

[432] LÓPEZ JIMÉNEZ, David: "Los sistemas de autodisciplina: presupuestos para su concurrencia", *Nuevas coordenadas para el Derecho de obligaciones. La autodisciplina del comercio electrónico*, 2013, Marcial Pons, p. 268.

[433] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing". *Derecho y cloud computing*, 2012, p. 193-194.

[434] Se recomienda el estudio de MERCHÁN MURILLO, Antonio: "Cloud computing: soluciones ante un posible conflicto de leyes", *Revista La Ley Mercantil*, 2018, nº48, junio 2018.

[435] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32008R0593. Último acceso: 08.08.2018.

en numerables ocasiones a lo largo del presente, que permita adecuar las necesidades a los requerimientos técnicos demandados y ofertados. Con la finalidad de evitar interpretaciones erróneas en los términos y facilitar el desarrollo de la actividad del prestador del servicio surgen en los contratos del *cloud* cláusulas específicas y anexos, principalmente el Acuerdo de Nivel de Servicio. En las cláusulas generales, subapartado anterior, se han recogido los condicionantes marcos que suelen aparecer en toda contratación empresarial. La simplificación en el proceso de contratación del servicio ("una parada", a través de un solo proveedor), la rapidez con la que se desarrolla y la necesaria seguridad de la tracción y de la prestación exigen un clausulado específico acorde. De este modo, determinar la responsabilidad de las partes, no solo por el incumplimiento de las obligaciones principales sino de la derivada del incumplimiento del ANS; la determinación de un uso aceptable de la tecnología a obedecer por el cliente y el usuario; la localización y tratamiento de los datos que se encuentran en la nube, con vinculación directa a la cláusula general de protección de datos; la confidencialidad y la seguridad en el servicio; y los cambios en las características del servicio, entre otras cláusulas que abordaremos, devienen fundamentales para una regulación completa del servicio de la nube. Aunque el ANS suele aparecer como anexo al contrato, por el desarrollo y los parámetros técnicos que contiene, vamos a tratarlos como un subíndice de las cláusulas específicas. Intentaremos discernir los condicionantes jurídicos afectos.

En reiteradas ocasiones se ha puesto de manifiesto la percepción general, para los clientes, de la dificultad en la alteración de los términos tipo del contrato de *cloud*. Las características y la dimensión de los clientes determinarán el poder negociador. De esta forma, las organizaciones pequeñas y medianas elegirán entre los distintos contratos que ofrecen, en el mercado, los proveedores del servicio, dada su escasa capacidad de negociación; y las grandes organizaciones dispondrán de la facultad de confeccionar, al menos en parte, las cláusulas que regirán la relación contractual. En ambos casos, la ENISA recomienda evaluar los contratos y los Acuerdos de Nivel de Servicios para responder a las cuestiones legales asociadas a la computación en la nube[436]. Los factores que más influyen en el desarrollo de las cláusulas contractuales (como proyección

[436] ENISA: "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009, p. 93. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

reguladora del servicio), por lo tanto, serán la demanda y la oferta dirigida, por lo que los términos predispuestos por los proveedores mejorarán con la demanda de los grandes usuarios, es decir, grandes corporaciones y con el uso del *cloud* en las Administraciones públicas.

i. Responsabilidad

El estudio del régimen de responsabilidad de las partes surge ante las eventualidades que pueden acontecer en el normal desarrollo de la relación contractual, riesgo que debe ser tratado en el contrato. La pérdida de información, los errores en el tratamiento o la parada del funcionamiento de la nube acaecen como alguno de los riesgos más comunes, aunque no únicos.

Los proveedores de servicios, sobre todo en referencia a las interrupciones y las pérdidas de datos, intentan excluir o restringir la responsabilidad asociada a los incumplimientos o eventualidades aparecidas en el desarrollo de la relación contractual tanto como sea posible. Aunque la determinación de la responsabilidad está presente en todos los órdenes jurisdiccionales, es cierto que es más proclive a su exclusión en la jurisdicción de EE.UU., curiosamente el ámbito geográfico donde más se determina la jurisdicción por los proveedores de servicios. Aunque los usuarios pueden negociar con éxito el sistema de responsabilidad del proveedor de los servicios, generalmente al relacionarse con un contrato con objeto amplio (por ejemplo, abastecimiento general en telecomunicaciones), en la mayoría de los contratos la responsabilidad del proveedor se limita a las pérdidas "directas", con los problemas subyacentes de la indeterminación del concepto. La "responsabilidad directa" puede definirse como las pérdidas económicas del cliente asociadas con las pérdidas o divulgación de los datos alojados en el servicio de *cloud*[437]. Incluso así, algunos proveedores intentan limitar la responsabilidad por daños directos en la medida de lo posible, ya sea en términos generales o en relación con las consecuencias de la incapacidad de acceder a los datos.

[437] BRADSHAW, Simon; MILLARD, Christopher y WALDEN, Ian: "Contracts for Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", *Queen Mary University of London - Legal Studies Research Paper*, 2010, nº 63, p. 33.

GOGRID[438], compañía del grupo DATAPIPE[439], en los términos del servicio recogía expresamente *"excepto en lo regulado particularmente en los ANS, y salvo que la ley específicamente aplicable prohíba la restricción de la responsabilidad por contrato, GOGRID no asumirá responsabilidad por reclamación, pérdida, acción, daño o demanda ante cualquier procedimiento resultante…"*[440]. Entre los riesgos comprendidos se encuentran las brechas de seguridad sin limitación, la exposición de cualquier dato o identificación personal, la pérdida de datos o de acceso a los mismos, las acciones de terceros, los errores o interrupciones, y las acciones de los empleados de GOGRID fuera del ámbito de sus funciones. Esta cláusula no se encuentra presente en otros servicios de la nube que ofrece la matriz. Tanto es así que, en los *purchase order terms and conditions*[441], documento marco para todos los servicios que ofrecen, establece que "*in no event shall Buyer be liable for any incidental, indirect, special, consequential or punitive damages, even if Buyer knew or should have known of the possibility of such damages"*[442].

La indemnización por responsabilidad contractual aparece reconocida en los artículos 1.101 y ss. del Código civil. Como se ha puesto de manifiesto, los proveedores tienden a excluir cualquier tipo de responsabilidad, por lo tanto, y a falta de unos criterios orientadores sobre la validez de las limitaciones de la responsabilidad[443], deberá valorarse

[438] TERMS OF SERVICE de GOGRID accesibles en: https://www.datapipe.com/gogrid/legal/terms-of-service. Última revisión de 22.11.2013 (Ref.: CGS_030417). Último acceso: 22.05.2017. Tras la compra de DATAPIPE, la web y los servicios están accesible pero no los términos legales (revisión 08.08.2018).

[439] El 11.09.2017 la compañía fue adquirida por RACKSPACE. Los términos continúan vigentes para los clientes antiguos, pero ya no son accesibles desde la web.

[440] Traducción libre. Cita literal: *"except to the extent specifically provided in the sla, and except to the extent that applicable law specifically forbids such restriction of liability by contract, gogrid will have no liability whatsoever for any claims, losses, actions, damages, suits, or proceedings resulting from any of the following or from any GOGRID efforts to address or mitigate any of the following…".*

[441] PURCHASE ORDER TERMS AND CONDITIONS de DATAPIPE, accesible en: https://www.datapipe.com/legal/purchase-order-terms-and-conditions. Versión 22.05.2017. Último acceso: 22.05.2017.

[442] Traducción libre: *"en ninguna circunstancia el comprador será responsable por daños incidentales, indirectos, especiales, significativos, ni deberá indemnizar por daños y perjuicios, incluso si el cliente conociera o debiera conocer la posibilidad de tales daños…".*

[443] Los *Unfair Contract Terms Act 1977*, de Reino Unido, regulan las cláusulas de exclusión y limitación de responsabilidad en el ordenamiento anglosajón. Accesible en: https://www.legislation.gov.uk/ukpga/1977/50. Último acceso: 08.08.2018.

el deber de diligencia del proveedor del servicio en la nube y la obligación legal que impone, en su caso, el ordenamiento jurídico[444].

HON, MILLARD y WALDEN[445] destacan cómo son los proveedores de servicio de menor tamaño los más propensos a aceptar un reparto equitativo de responsabilidad en el incumplimiento del servicio. Detectan, en concreto, que los proveedores *SaaS* aceptan asumir la responsabilidad por las interrupciones del servicio si el fallo proviene de la conectividad a Internet en sus centros de datos. Sin embargo, son reacios a incluir todos los riesgos asociados a las licencias de *software* utilizado, justificando esta medida en el objeto de su actividad, es decir, señalan que sus acciones empresariales van destinadas a prestar servicios de computación en la nube, no a ser meros intermediarios en la concesión de licencias. Por ello, las penalidades asociadas a la responsabilidad en materia de propiedad intelectual e industrial se encuentran limitadas y solo son asumidas en caso de pérdidas directas.

A pesar de su parca redacción, a efectos expositivos podemos valernos de las CONDICIONES PARTICULARES DEL SERVICIO SMART IB[446] de ACENS. Definido como servicio en la nube que permite "*una solución plug&play de Business Intelligence"* basadas en un *software* proporcionado por la compañía, establece que "*respecto del software que no haya sido licenciado por acens, será responsabilidad del CLIENTE cualquier tipo de reclamación por, entre otras cosas, la adquisición y mantenimiento de las licencias de cualquier aplicación software instalado de acuerdo a las condiciones acordadas con el fabricante del software"*. ZOHO para su servicio CREATOR[447], siendo consciente del problema que entraña la conectividad del servicio en los productos *SaaS*, y excluyendo su responsabilidad ante cualquier interrupción en

[444] El artículo 1.101 del CC habla de actuación dolosa, negligente o morosa del proveedor; el artículo 1.106 del CC incorpora el lucro cesante en la indemnización, y el artículo 1.107 del CC hace referencia a los perjuicios como consecuencia directa de su falta de cumplimiento. Hay que tener presentes, además, las disposiciones generales en el régimen de contratos que ordena el Código.

[445] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 11-12.

[446] CONDICIONES PARTICULARES DEL SERVICIO SMART IB de ACENS. Accesible en: https://www.acens.com/file_download/Condiciones_particulares_de_Servicio_Smart_Bi.pdf. Versión de 08.08.2018. Último acceso: 08.08.2018.

[447] Más información en: https://www.zoho.eu/creator/. Último acceso: 08.08.2018.

sus sistemas por conexión e interrupciones[448], pone a disposición de los clientes un *software* de trabajo *offline* que conecta con el servicio de la nube cuando se restablezca la conexión.

Cuando la exención de responsabilidad no entra en juego, es probable que esta se encuentre limitada a los recursos económicos aportados por el cliente. De esta forma, suele establecerse unos topes máximos relacionados con la cantidad pagada por el usuario para la prestación del servicio, ya sea en su totalidad o por un período de tiempo. En nuestro ordenamiento jurídico, como hemos indicado, el artículo 1.106 del CC incorpora el abono del lucro cesante a los datos y perjuicios causados, en concepto de indemnización.

IBM, para el servicio BLUEMIX[449], establece como única compensación posible al cliente el resarcimiento mediante créditos a satisfacer en futuras facturaciones del servicio, pudiendo no reconocer el 100% de la indisponibilidad de la nube. Sin embargo, la cláusula más relevante es la establecida por SAP para todos sus servicios de la nube[450]. Reconoce que *"la única solución del Cliente y la responsabilidad completa de SAP"* será prestar otra vez el servicio realizado de forma deficitaria o "*si SAP no puede volver a prestar el Servicio Cloud, el Cliente podrá terminar su suscripción al Servicio Cloud afectado. Toda terminación debe darse en un plazo de tres meses después de que SAP no haya sido capaz de volver a prestar el Servicio Cloud"*. Nada dice sobre los perjuicios que le supone al cliente, no solo por la deficiencia del servicio, sino por la terminación anticipada del contrato.

Ya hemos comentado que dentro de los regímenes de responsabilidad en el uso de la nube podemos diferenciar dos tipos: el general, establecido para el supuesto de incumplimiento de cualquiera de las obligaciones contenidas en el contrato, y el régimen

---

[448] Exclusiones recogidas en ZOHO CREATOR TERMS OF USE (versión vigente a 08.08.2018), accesible en https://www.zoho.com/creator/terms.html, como en TERMS OF SERVICE de ZOHO (versión 19.04.2015, vigente a 08.08.2018), accesible en https://www.zoho.eu/terms.html.

[449] Descripción del servicio accesible en: https://www.ibm.com/cloud-computing/bluemix/sites/default/files/assets/docs/i126-6605-12_11-2017_en_US.pdf_0.pdf. Versión i126-6605-1 (11/2017). Último acceso: 08.08.2018.

[450] Se puede acceder a los TÉRMINOS Y CONDICIONES GENERALES PARA SAP CLOUD SERVICES en: https://assets.cdn.sap.com/agreements/general-terms-and-conditions/cls/general-terms-and-conditions-for-sap-cloud-services-direct-spain-spanish-v2-2017.pdf. Versión v.2-2017. Último acceso: 26.05.2017.

de responsabilidad por incumplimiento de lo contenido en el Acuerdo del Nivel de Servicios. El régimen de responsabilidad del ANS difiere del régimen de responsabilidad por incumplimiento de las obligaciones contractuales. El primero hace referencia, exclusivamente, a la inobservancia de lo establecido en el Acuerdo del Nivel de Servicios, mientras que el segundo hace alusión al incumplimiento contractual general[451]. Será en el deficiente cumplimiento del Acuerdo del Nivel de Servicio donde se reconozca, de manera más estandarizada, algún tipo de responsabilidad por parte del proveedor del *cloud*.

Es oportuno, en el estudio de la responsabilidad en los servicios en la nube, atender a las recomendaciones expuestas por la ENISA[452] ante la contratación de los servicios de computación en la nube. Determina para cada tipo de servicio, cliente y proveedor quién debe ser responsable en función de las características del modelo de implantación. Si el cliente no puede negociar las cláusulas contractuales se recomienda analizar detenidamente el ámbito de sus responsabilidades.

Cuando la modalidad del servicio es *SaaS*, así se ha visto en la práctica, el cliente debe ser responsable del cumplimiento de la ley de protección de datos respecto a los datos recabados y procesados, del mantenimiento del sistema de gestión de identidad, de la gestión del sistema de identidad y de la gestión de la plataforma de autentificación (así como del cumplimiento de las políticas de contraseñas). Como contrapartida, el proveedor del servicio debe asumir la responsabilidad sobre el mantenimiento de las infraestructuras de soporte físico, la disponibilidad y seguridad de las infraestructuras físicas (servidores, almacenamiento, red…), la gestión de parches del sistema operativo y procedimientos de refuerzo, de la verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor, la configuración de la plataforma de seguridad, la supervisión de los sistemas, el mantenimiento de la plataforma de seguridad (antivirus, cortafuegos, filtrado de paquetes…) y de la recogida de registros y control de seguridad.

---

[451] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing". *Derecho y cloud computing*, 2012, p. 198-199.

[452] ENISA: "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009, p. 71-77. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

La realidad, sin embargo, dista mucho de la teoría. Los pequeños y medianos clientes raramente podrán beneficiarse de este equilibrio de responsabilidades. Ya se ha expuesto cómo un gran proveedor, ZOHO, excluye gran parte de las responsabilidades que debería asumir un proveedor *SaaS*.

Cuando se presta el modelo de plataforma como servicio, *PaaS*, el cliente debe responder del mantenimiento del sistema de gestión, la gestión del sistema de identidad y la gestión de la plataforma de autentificación (incluido la política de contraseñas). El proveedor de servicios debe asumir mayor responsabilidad, dada las características del servicio, debiendo ser responsable de las infraestructuras de soporte físico, la disponibilidad y seguridad de las infraestructuras físicas, la gestión de parches del sistema operativo y procedimientos de refuerzo, la verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor, la configuración de la plataforma de seguridad, la supervisión de los sistemas, el mantenimiento de la plataforma de seguridad y la recogida de registros y control de seguridad.

Por último, cuando la nube se configura como *IaaS,* el cliente puede asumir más responsabilidad en la configuración del servicio, dado que tiene más control sobre el desarrollo y la viabilidad de la nube. De este modo, el cliente podría asumir la responsabilidad de la gestión y mantenimiento del sistema de gestión de identidad, la gestión de la plataforma de autentificación (así como del cumplimiento de las políticas de contraseñas), la gestión de parches del sistema operativo de invitado y procedimientos de refuerzo, la verificación de cualquier conflicto entre el procedimiento de refuerzo del cliente y la política de seguridad del proveedor, la configuración de la plataforma de seguridad de invitado, la supervisión de los sistemas de invitado, el mantenimiento de la plataforma de seguridad y la recogida de registros y control de la seguridad. Por el contrario, el proveedor de servicios debe asumir la responsabilidad de la disponibilidad y seguridad de las infraestructuras física, los sistemas de alojamiento y las óptimas condiciones de la infraestructura de soporte físico.

Estas recomendaciones tratan de establecer un reparto de responsabilidad equilibrado entre los clientes y los proveedores de computación en la nube, sobre la base del poder y control que cada una de las partes tienen sobre el servicio. Sin embargo, la constatación fáctica de las cláusulas que regulan la contratación y desarrollo del servicio distan de las directrices marcadas. Se extrapola un régimen de responsabilidad cercano al servicio *IaaS*

para todos los servicios de la nube, recayendo en el cliente compromisos fuera de su propio ámbito de actuación y control.

Un último inciso debemos realizar. Si el cliente del servicio *IaaS* es responsable de la seguridad en las infraestructuras, debe tenerse en cuenta que los proveedores tratarán las aplicaciones de la instancia virtual del cliente como una "caja negra", por lo que los clientes asumirán toda la responsabilidad de las aplicaciones alojadas en la nube.

Respecto a la responsabilidad en la subcontratación del servicio, no existe en nuestro ordenamiento jurídico obligación por la cual el proveedor principal tenga que responder del subproveedor ante el cliente. Si bien, sí puede atenderse al régimen de responsabilidad extracontractual, conforme al 1.902 y ss. del Código civil, pudiendo, posteriormente, el proveedor principal repetir los importes satisfechos[453].

ii. Uso aceptable

Sustancialmente similares en todos los proveedores de servicios, los "usos aceptables" vienen a imponer reglas de actuación a los clientes, buscando los proveedores liberarse de la responsabilidad derivada de las actuaciones realizadas por aquellos[454]. Esta cláusula debe ser, por tanto, estudiada y entendida a la luz del acuerdo completo entre las partes, principalmente con la regulación de la propiedad intelectual e industrial, la responsabilidad de las partes y las relacionadas con la protección de datos personales. No podemos olvidar que su cumplimiento se configura como una de las obligaciones del cliente.

Presentado comúnmente como AUPs (*Acceptable Use Policy*), algunos proveedores incluso la enmarcan en un anexo al contrato, prohibiendo un conjunto coherente de actividades que los proveedores consideran como indebidas o ilegales en la prestación del servicio. La mayor o menor extensión del documento está relacionada con el nivel de detalle con el que describen las actividades ilícitas. Las actividades prohibidas más comunes son la utilización de correo comercial no solicitado, actividades relacionadas con el fraude, utilizar el servicio como base a la piratería (contra la propiedad intelectual

[453] En materia de protección de datos personales nos emplazamos al régimen estudiado en el Capítulo IV.b.b.

[454] BRADSHAW, Simon; MILLARD, Christopher y WALDEN, Ian: "Contracts for Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", *Queen Mary University of London - Legal Studies Research Paper*, 2010, nº 63, p. 19-20.

o industrial), alojar contenidos obscenos o difamatorios, o que promuevan la discriminación o inciten al odio.

TERREMARK[455], compañía que ha sido adquirida por VERIZON, en sus servicios de *cloud computing* establecía una escueta regulación de los usos aceptables por el usuario:

"A través de su cuenta declara que no viola o infringe los derechos de terceros, incluidos los derechos de autor, marca comercial, privacidad u otros derechos personales y de propiedad y que no contiene material injuriante, difamatorio ni de otro modo ilícito. Acepta también no recolectar ni reunir direcciones de correo electrónico u otra información de contacto de los usuarios desde el Sitio web por medios electrónicos o de otro tipo. Además, acepta no usar secuencias de comandos automáticas para recopilar información del Sitio web o con cualquier otro fin. También acepta no usar el Sitio web de ninguna manera ilegal o de cualquier otra forma que pudiera dañar, desactivar, sobrecargar o afectar al Sitio web. Asimismo, usted acepta no usar el Sitio web para:

- *cargar, publicar, enviar por correo electrónico transmitir o de otro modo poner a disposición cualquier contenido que consideremos dañino, amenazador, abusivo, acosador, vulgar, obsceno, cargado de odio o que sea objetable desde un punto de vista racial o étnico, ni intimidar o acosar a otro usuario del Sitio web.*
- *hacerse pasar por otra persona o entidad, o tergiversar una declaración o de otro modo falsificar su identidad o su afiliación con otra persona o entidad*
- *cargar, publicar, enviar por correo electrónico, transmitir o de otro modo poner a disposición cualquier material que contenga virus de software u otro código, archivos o programas informáticos diseñados para interrumpir, destruir o limitar la funcionalidad de cualquier software o hardware o equipo de telecomunicaciones.*
- *usar o intentar usar la cuenta, servicio o sistema de otra persona sin autorización de Terremark, o crear una identidad falsa en el Sitio web".*

[455] CONDUCTA DEL USUARIO de TERREMARK.ES, versión 09.2013. Era accesible a través de la dirección: http://www.terremark.es/legal-notices.aspx. A fecha de 08.08.2018 no se encuentra disponible la web del proveedor, tras la compra por VERIZON.

VERIZON[456] ahora trata la *Acceptable Use Policy* de manera particularizada, estableciendo una reglamentación diferenciada del cuerpo *terms and conditions*, si bien, coincide en lo esencial con lo establecido por TERREMARK, salvo en la regulación expresa del acceso o uso no autorizado de datos, sistemas o redes para salvaguardar las medidas de seguridad de la red y del sistema del propietario[457].

Más oportuna parece la utilización de la AUP para reglamentar las actividades permitidas dentro del concreto objeto del contrato, de esta forma complementará su definición. Sirva de ejemplo la prohibición del uso de la nube para otro fin que no sea realizar copias de seguridad de los datos de la empresa, o la limitación del acceso y utilización de algunos usuarios en función de área geográfica de procedencia, principalmente debido a razones de seguridad o de bloqueo comercial.

Aunque difuso en sus TERMS OF SERVICE, no establece una cláusula de AUP diferencia, es oportuno ver cómo ADRIVE[458] imposibilita sus servicios a los ciudadanos y empresas residentes o establecidas en diferentes países:

"Ningún servicio de almacenamiento debe ser adquirido por un exportador o re-exportador (contratista y subcontratista es el término empleado en nuestro trabajo) *por nacionales o residentes en Cuba, Irán, Iraq, Libia, Corea del Norte, Siria o Sudán o cualquier otro país en los que EE.UU. haya establecido políticas de embargo; o cualquier persona incluida en U.S. Treasury Department's list of Specially Designated Nationals, así como las personas bloqueadas, y los incluidos en the U.S. Commerce Department's*

[456] ACCEPTABLE USE POLICY para los servicios de la nube y soluciones IT de VERIZON, accesible en: http://www.verizonenterprise.com/terms/aup/. Versión de 08.08.2018. Último acceso: 08.08.2018.

[457] De forma literal establece: *"Violations of system or network security are prohibited, and may result in criminal and civil liability. Verizon will investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:*
Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network.
Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network.
Interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks.
Forging of any TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting".

[458] Se puede acceder a los TERMS OF SERVICES de ADRIVE en: http://www.adrive.com/terms. Última actualización: 22.09.2015 (Vigentes a 08.08.2018). Último acceso: 08.08.2018.

Table of Denial Orders. Como usuario o cliente del servicio declara y garantiza que no se encuentra bajo el control, o no es nacional o residente, de alguno de los países de la lista…"[459].

Un ejemplo claro de cómo puede ayudar a clarificar el objeto del contrato, facilitar la interpretación de las cláusulas contenidas y el poder decisorio de las partes es el aportado por APONTE SYSTEMS[460]. Definiendo cuál es su uso apropiado establece que *"el Web Hosting, Cloud Hosting y VPS Hosting está diseñado para servir las necesidades de alojamiento web, email, base de datos MySQL y DNS de pequeñas y medianas empresas, de propiedad independiente. No es apropiado utilizar nuestros servicios para apoyar a las grandes empresas o negocios a nivel internacional a base de una demanda sostenida que coloca una carga excesiva en nuestros sistemas o impactos negativamente a utilizar por las empresas pequeñas o medianas, de propiedad independiente y operado"*. Con esta pequeña aportación el cliente puede clasificar al proveedor de servicios y determinar si sus necesidades se adecúan a un sistema de *cloud* con servidores compartidos y que no facilita el *hosting* continuado de grandes archivos electrónicos. Este proveedor incluso establece la posibilidad de suspender el servicio, previa comunicación al cliente, si se utiliza un porcentaje de recursos de los CPUs, se ejecuta *software* con IRC o servicios de intercambio de datos (tipo P2P), incluso si sirve como servidor para juegos en línea[461].

iii. Localización y tratamiento de los datos

La localización y el tratamiento de datos se ha tratado de forma holística en el Capítulo IV y en *"las condiciones generales en el contrato del cloud computing"*. En todo este desarrollo hemos manifestado la importancia que tienen en los contratos empresariales de los servicios de *cloud* la regulación específica de lo ateniente al

---

[459] Traducción libre. Cita literal: *"No Storage Data shall be acquired by or otherwise exported or re-exported into (or by or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Syria, Sudan or any other country to which the U.S. has embargoed goods; or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals and Blocked Persons or the U.S. Commerce Department's Table of Denial Orders. As a Storage Data Recipient and/or User, You represent and warrant that You are not located in, under the control of, or a national or resident of any such country or on any such list"*.

[460] POLÍTICA DE USO JUSTO (AUP) de APONTE SYSTEMS. Accesible en: https://aponte-systems.com/secure/Politicas/Uso_Aceptable, versión 3.1.8E. Último acceso: 08.08.2018.

[461] Aunque la sociedad tiene domicilio social en México y la regulación de su política de uso se redacta conforme a la legislación vigente en ese país, recomendamos su lectura y estudio por las particularidades y el detalle que presenta.

tratamiento de los datos personales. Una regulación adecuada potenciará el correcto funcionamiento del servicio, por lo tanto, la cláusula contractual deberá identificar de manera concisa al responsable del fichero de datos en cuestión y quién actuará como encargado del tratamiento. De igual forma, debería incluir las medidas de seguridad a las que debe acogerse el responsable del tratamiento, conforme al RGPD y RLOPD si es aplicable la legislación española, y tratar de forma precisa las transferencias internacionales de datos de carácter personal, ya sea con destino a países de la Unión Europea, de protección equiparable o hacia terceros países que no gozan del amparo del RGPD. Por ello, en los contratos de computación en la nube los proveedores deberían dar a conocer todas las ubicaciones de sus centros de datos, incluso aquellos que utilizan para realizar copias de seguridad, estableciéndose de manera certera la posibilidad, o no, de exportación de los datos fuera del EEE. Es más, a la luz del RGPD y la nueva figura del delegado de protección de datos, que tiene entre otras misiones asesorar al responsable o al encargado de datos en todo lo relativo a la normativa aplicable, y que puede recaer en personal interno de la entidad de tratamiento o en personal externo, es oportuno recoger la designación de la figura, aunque posteriormente un contrato entre las partes regule su actuación. El RGPD declara que los datos de contactos deben hacerse públicos por los responsables y encargados[462].

Los clientes deben conocer qué localización tienen los centros de datos del proveedor, no solo para estudiar las restricciones en las transferencias de datos personales fuera del EEE, sino para cerciorarse de que los controladores eligen procesadores de datos que garantizan de manera suficiente las medidas de seguridad requeridas[463]. No puede olvidarse la responsabilidad que tiene el cliente en la elección del proveedor de la nube, vigente el RGPD. Serán los proveedores de servicios quienes puedan solucionar los problemas relacionados con la localización de los centros de datos mediante el uso de nubes privadas o alianzas entre proveedores, ofreciendo a los clientes la posibilidad de

[462] Para un conocimiento exacto de la figura del Delegado de Protección de Datos recomendamos el estudio del trabajo realizado por Grupo de Trabajo del artículo 29 sobre protección de datos, titulado "Directrices sobre los delegados de la protección de datos (DPD)", del 13 de diciembre de 2016. Accesible en: https://www.aepd.es/media/criterios/wp243rev01-es.pdf. Último acceso: 08.08.2018.

[463] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 18.

determinar dónde quieren localizar sus datos. El problema es que requerirán más recursos, lo que redundará en mayores costes asociados al servicio.

SALESFORCE, proveedor de servicios para empresas, entre ellos la nube, establece una herramienta, SALESFORCE TRUST[464], para comprobar en tiempo real la ubicación de tus datos entre los distintos centros disponibles de Asia, Europa y América, así como el número de incidentes, el rendimiento del sistema y las prácticas de seguridad adoptadas, entre otros aspectos.

Otra razón para conocer la localización de los datos personales a tratar es garantizar la confidencialidad. No se puede obviar los hechos acontecidos en 2013 cuando Microsoft, Apple, Facebook, Yahoo, Google, PalTalk, AOL, Skype y YouTube, entre un largo etcétera, reconocieron que permitieron al Gobierno de EE.UU. entrar en sus servidores, a través del programa de espionaje *PRISM,* amparados por la *USA Patriot Act*, fundamentando la medida en la investigación contra el terrorismo internacional[465]. Ya en 2013 The Guardian aventuraba que la cesión de datos por los grandes proveedores tecnológicos tenía como fundamento una compensación económica[466].

El conocimiento de la localización de los centros de datos debe extenderse a todas las unidades de los sujetos que intervienen en la relación contractual, es decir, no solo a los centros de datos de los dependientes de forma directa por los proveedores del servicio, sino de los terceros relacionados que prestan apoyo al principal. Esta subcontratación puede suponer un acceso a los metadatos o datos de la empresa cliente por subproveedores en territorios con una laxa seguridad. Por lo tanto, determinar en el contrato de la nube la localización, si se recoge la posibilidad de la subcontratación del servicio, de los centros de los subcontratistas es requisito necesario y más cuando su ubicación previsible sea fuera del EEE.

---

[464] SALESFORCE TRUST es accesible en: https://trust.salesforce.com/es/. Último acceso: 08.08.2018.

[465] Cinco Días (edición digital): "La ley patriota de EE UU castiga a las tecnológicas", 2013, noticia de 17.06.2013. http://cincodias.com/cincodias/2013/06/16/empresas/1371398022_860080.html. Último acceso: 08.08.2018.

[466] The Guardian (edición digital): "NSA paid millions to cover Prism compliance costs for tech companies", 2013, noticia de 23.08.2013. http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid. Ultimo acceso: 08.08.2018.

Práctica común en los proveedores es recoger la ubicación de los centros de datos sin determinar exactamente dónde se ubicarán los datos. Este es el caso de INTEROUTE[467], si bien, puede accederse a una ficha técnica que recoge todas las circunstancias que atienden al alojamiento físico. ARSYS en la contratación de los servicios de la nube permite configurar la contratación en *data centers* de España o en EE.UU.[468].

En referencia al tratamiento de datos es de especial importancia establecer la obligación de hacer constar cualquier subencargo de tratamiento, dado que puede entrar en juego un nuevo actor en la relación contractual. Independientemente de si esta subcontratación conlleva el procesamiento de datos personales, puede ser oportuno restringir contractualmente por el cliente la subcontratación, incluso del personal de apoyo, o, al menos, que sea necesario el consentimiento expreso del cliente. Una alternativa puede ser que el subcontratista seleccionado provenga de una lista de proveedores pre-aprobada por el cliente de la nube y bajo una serie de condiciones predispuestas.

En el CLOUD SERVICES AGREEMENT[469] de IBM, el proveedor puede utilizar "personal y recursos" de todo el mundo, incluyendo a terceros contratistas y subprocesadores para llevar a cabo los servicios en la nube, si bien establece una lista de países donde puede distribuirse los servicios del *cloud*, proveyendo a los clientes una lista actualizada de proveedores en el momento del contrato si lo solicita, y siendo IBM responsable de lo acordado en el documento, incluso si terceras partes intervienen en la prestación del servicio[470]. TREVENQUE, entidad española propietaria del Cloud Center

---

[467] Podemos acceder a los centros de datos de INTEROUTE en http://www.interoute.es/empresas/infraestructura/colocation. Incluye, además, las certificaciones que ostentan los centros de datos y otras características, como ubicación, conectividad o seguridad, entre otros.

[468] Aunque en la web ARSYS, al menos de acceso público sin necesidad de finalizar el proceso de contratación, no establece dónde se localizan los alojamientos de datos en España, DATA CENTER MAPS nos permite situarlo en Logroño. Accesible en: http://www.datacentermap.com/spain/logrono/arsys.html. Último acceso: 08.08.2018.

[469] CLOUD SERVICES AGREEMENT de IBM, versión Z126-6304-US-8, 03-2018, accesible en: https://www-05.ibm.com/support/operations/files/pdf/csa_us.pdf. Último acceso: 08.08.2018.

[470] De forma literal: *"IBM may use personnel and resources in locations worldwide, including third party contractors and subprocessors to support the delivery of the Cloud Services. IBM may transfer Content, including personally identifiable information, across country borders. A list of country where Content may be rpocessed for a Cloud Service is avaible at www.ibm.com/cloud/datacenters or as described in the Attachment or TD. IBM is responsible for the obligations under the Agreement even if IBM uses a third party contractor or subprocessors unless otherwise set forth in a TD. IBM will require subprocessors with access to Content to maintain technical and organizational security measures that will enable IBM to meet*

Andalucía, recoge en las CONDICIONES GENERALES DE CONTRATACIÓN[471] que *"*(debe) *comunicar en su caso al CLIENTE, el nombre de la entidad o profesional al que se le encomienden tareas que puedan implicar el acceso o tratamiento de los datos de carácter personal propiedad del CLIENTE"* para los supuestos de subcontratación, autorizada por el cliente si acepta las condiciones generales de contratación.

Un aspecto que pocos proveedores tratan es la seguridad de los datos en tránsito, muy relacionado con la localización de los centros de datos, dado que a menos que el proveedor de servicios haya construido o alquilado su propia red y haya establecido sistemas de seguridad, las transferencias entre los centros de datos suelen hacerse a través de Internet.

La mayoría de los proveedores de la nube suelen establecer una cláusula similar a la recogida por UKFAST en su PRIVACY POLICY[472], que en el apartado referente a la información sobre la seguridad de los servicios recoge *"please be aware that communications over the Internet, such as emails/web mails, are not secure unless they have been encrypted. Your communications may route through a number of countries before being delivered - this is the nature of the World Wide Web/Internet. UKFast cannot accept responsibility for any unauthorised access or loss of personal information that is beyond our control"*[473]. Sin embargo, como ya dijéramos en el Capítulo IV.b.a, DROPBOX[474] reconoce y establece un sistema de cifrado seguro para los datos en

its obligations for a Cloud Service. A current list of subprocessors and their roles will be provided upon request".

[471] CONDICIONES GENERALES DE CONTRATACIÓN de GRUPO TREVENQUE. Accesible en: https://www.trevenque.es/wp-content/uploads/2017/03/01.-condiciones-legales-contratacion.pdf. Último acceso: 08.08.2018.

[472] PRIVACY POLICY de UKFAST, versión de 04.07.2018, accesible en: https://www.ukfast.co.uk/terms/privacy-policy.html. Último acceso: 08.08.2018.

[473] Traducción libre: *"tenga en cuenta que las comunicaciones a través de Internet, como el email y las webs mails, no son seguras salvo que se hayan encriptado/cifrado. Tus comunicaciones pueden atravesar distintos países antes de ser entregadas al destinario – esta es la tecnología empleada por WWW/Internet. UKFAST no asume la responsabilidad ante el acceso no autorizado o la perdida de información personal fuera de nuestro control".*

[474] DROPBOX BUSINESS SECURITY, A DROPBOX WHITEPAPER, versión v2017.04. Accesible en: https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf. Último acceso: 08.08.2018.

tránsitos y *at rest*, no solo cuando se actúa bajo navegadores sino también con aplicaciones de escritorio o móviles[475].

Para finalizar, aunque pudiera estar presente en otras cláusulas del contrato, debe determinarse también aquí si el proveedor de la nube actúa como procesador de datos de forma activa y cuáles son sus responsabilidades. Habrá que revisar y determinar el papel exacto del proveedor de la nube en cada caso, a fin de evaluar si actúa como agente procesador de datos, y si es así, si además actúa como controlador de datos con una finalidad propia[476]. Debe garantizarse, además, que el proveedor de servicios no utiliza los datos aportados por el cliente con propósitos distintos, es decir, no procesa datos con fines distintos que los de la mera prestación del servicio requerido.

iv. Seguridad en el servicio

La seguridad en la computación en la nube es uno de los condicionantes más relevantes a la hora de implantar el servicio en el entorno empresarial, no solo por las preocupaciones en la pérdida del control de los datos almacenados en la nube sino por la correcta aplicación de las medidas establecidas en la normativa de control. El estudio de las medidas de seguridad en una fase precontractual dependerá en gran medida del modelo de servicio en nube contratado. Como ya indicáramos en el estudio de la responsabilidad, los clientes tienen un mayor control en las medidas de seguridad cuando el modelo se configura como *IaaS* y *PaaS*, mientras que en el modelo *SaaS* serán los proveedores quienes ostenten un mayor control sobre el *cloud*.

Los usuarios pueden exigir auditorías que analicen la seguridad física y digital, antes incluso de la propia celebración del contrato, para garantizar que el suministrador del servicio tiene establecidas políticas y sistemas de seguridad adecuados, así como un proceso de actuación apropiado, no solo referente a los datos personales sino de forma

[475] Expresamente se establece: *"To protect data in transit between Dropbox apps and our servers, Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a Dropbox client (currently desktop, mobile, API, or web) and the hosted service is always encrypted via SSL/TLS. For end points we control (desktop and mobile) and modern browsers, we use strong ciphers and support perfect forward secrecy and certificate pinning. Additionally, on the web we flag all authentication cookies as secure and enable HTTP Strict Transport Security (HSTS) with includeSubDomains enabled"*.

[476] En el Capítulo IV tratamos de forma holística la actuación del proveedor de servicios en la nube con el fin de evaluar su actuación en el tratamiento de los datos personales del cliente y de los usuarios.

global al servicio. Mayor garantía para el cliente, y mayor confianza en el servicio y en el proveedor seleccionado, será determinar y recoger las políticas y sistemas de seguridad que aplicaron ante un problema determinado en un período previo a la contratación.

Que un sujeto independiente a la relación contractual lleve a cabo una auditoría de seguridad del servicio y que el proveedor ponga a disposición del cliente una copia de la evaluación, permite tomar una decisión informada, al conocer medidas de disponibilidad, confidencialidad e integridad (lo que incluye medidas técnicas, físicas y organizativas) que ofrece el proveedor de servicios[477]. ENISA resalta que el contrato debería especificar claramente las condiciones de las pruebas independientes o del cliente, estableciendo los sistemas o componentes del sistema sobre los que recaerá y qué tipo de pruebas se llevarán a cabo[478].

Sin embargo, como se indica en el estudio de HON, MILLARD y WALDEN[479], los proveedores suelen ser reacios a proporcionar información sobre su política y las medidas de seguridad empleadas, sobre todo con una infraestructura compartida o en un entorno multiempresa, porque dicho estudio de transparencia podría comprometer la seguridad de los usuarios, presentes o potenciales. Alegan, además, que podrían revelar información sensible (la descripción de vulnerabilidades puede incluir información confidencial y/o comercial)[480]. Por lo tanto, la posibilidad de tener un conocimiento detallado e

[477] INFORMATION COMMISSIONER'S OFFICE (ICO): "Guidance on the use of cloud computing: Data protection act 1998", 2012, v. 1.1., p.13.

[478] ENISA: "Procure Secure: A guide to monitoring of security service levels in cloud contracts", 2012 (April), p. 37. Accesible en: https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport. Último acceso: 08.08.2018.

[479] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 25.

[480] ENISA plantea como posibilidades, con el fin de solventar los problemas que tiene revelar información sobre vulnerabilidades, las siguientes:

- Si se ejecuta un *software* personalizado, desarrollado, dirigido y operado internamente por el proveedor de servicios (como parte de la prestación del servicio) se podría informar sobre el número de vulnerabilidades corregidas o parcheadas, después de hacer público el informe de vulnerabilidades. Además, podría relacionarse dicha información por períodos.
- Cuando el *software* proceda de un tercero ajeno a la relación contractual, las vulnerabilidades serán detectadas y denunciadas por el tercero, debiendo el proveedor de servicios analizar la información suministrada e indicar cómo se ve afectado y el impacto de dichas vulnerabilidades en el servicio que ofrece.
- Cuando el desarrollo del *software* se ejecute en un entorno profesional (modelos *IaaS* y *PaaS*), el proveedor podría ofrecer un servicio de advertencias o de alertas sobre vulnerabilidades y

información sobre las medidas de seguridad dependerá, nuevamente, de la capacidad de negociación del cliente, siempre bajo pacto de confidencialidad, así como de la documentación específica que otorgarían diferentes certificaciones, como por ejemplo la ISO27001[481].

IBM BLUEMIX, por ejemplo, publicita que cumple con las principales certificaciones ISO, así como con los estándares que dictaminan FedRAMP, FISMA, es miembro de EU-US Privacy Shield Framework y cumple con las cláusulas modelos que establece la Unión Europea[482].

Las posibilidades de que el cliente imponga al proveedor del servicio las medidas de seguridad que considere adecuadas, *ex contractu,* dependerán del uso exclusivo o compartido de las infraestructuras con otros usuarios. Si los clientes requieren medidas adicionales de seguridad, por encima de los límites que establece la política de seguridad de los proveedores, ante datos sensibles, deberán baremar los costos adicionales que supone. De igual forma, el proveedor estudiará el sacrificio en el que incurrirá para obtener y mantener certificaciones que aseguren el nivel requerido. El acuerdo contractual deviene esencial. Más fácil lo tienen los clientes que satisfacen sus necesidades ante servicios estándares, debiendo prestar atención a certificaciones independientes de instituciones del sector como garantía del cumplimiento de los requisitos de seguridad por el proveedor. Cloud Security Alliance, Open Data Center Alliance y Cloud Industry Forum son algunas instituciones que están desarrollando estándares específicos para el *cloud*[483].

---

parches ejecutados por terceros, así como un servicio de verificación de seguridad para aplicaciones personalizadas.
Para más información véase: ENISA: "Procure Secure: A guide to monitoring of security service levels in cloud contracts", 2012 (April), p. 34-39. Accesible en: https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport. Último acceso: 08.08.2018.

[481] En el Capítulo IV.b.a. recomendábamos las ISO/IEC 27018:2014, o al menos las ISO/IEC 17065/20112, para la correcta aplicación del Reglamento europeo de protección de datos personales.

[482] Puedes acceder a la información completa de las certificaciones de IBM BLUEMIX en: https://www.ibm.com/cloud-computing/bluemix/es/compliance. Último acceso: 08.08.2018.

[483] Para más información véase: https://cloudsecurityalliance.org/, http://www.opendatacenteralliance.org/ y http://www.cloudindustryforum.org/.

Una medida que puede ser de gran utilidad para los clientes, y que puede recogerse en las cláusulas contractuales, son los derechos de auditoría o registros en el desarrollo de la prestación del servicio (antes hacíamos alusión a la auditoría general y precontractual del proveedor, no particular del servicio del cliente). El ICO recomienda un continuo seguimiento, revisión y evaluación del servicio por los clientes, para cerciorarse de que el servicio en nube funciona de la manera adecuada, como estipula el acuerdo contractual[484]. Algunos proveedores de servicios en nube han puesto en marcha herramientas que permiten a los clientes controlar el acceso a los datos, así como el monitoreo en tiempo real, lo que permite verificar quién accede a los datos, a qué accedieron y qué acciones ejecutaron[485]. Aunque es una medida que intenta aumentar la transparencia para el cliente del servicio, propiciando transparencia interpartes e intrapartes, el principal escollo puede provenir de la capacidad del proveedor de servicio para localizar y ubicar exactamente a los usuarios finales, más complejo en el supuesto de subcontratación por el proveedor de servicios, que puede no tener los derechos o control suficientes para el correcto funcionamiento de la herramienta planteada.

En las CONDICIONES ESPECÍFICAS[486] para CLOUDBUILDER NEXT se establece que *"el cliente podrá activar el servicio de monitorización para sus servidores. Se trata de una herramienta gratuita que permite configurar los recursos y servicios a monitorizar por servidor, así como los umbrales de alarma para cada uno de ellos, los cuales en caso de superarse enviarían un mensaje al correo electrónico indicado previamente por el cliente, informando sobre el umbral superado para el recurso y servidor afectados. Dispone de un histórico de datos y avisos generados durante el último año y permite importar y/o exportar la política de monitorización entre servidores…"*. Sin embargo, como la nube de MICROSOFT AZURE, el proveedor traslada toda la

[484] INFORMATION COMMISSIONER'S OFFICE (ICO): "Guidance on the use of cloud computing: Data protection act 1998", 2012, v. 1.1., p.11.

[485] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 28-29.

[486] CONDICIONES ESPECÍFICAS de la nube CLOUDBUILDER NEXT de ARSYS, Ref.: CECBN_141217. Accesible en: https://www.arsys.es/legal?dhtml=contrato-ngcs. Último acceso: 08.08.2018.

responsabilidad, indicando que no supervisará ni responderá dentro del área del cliente[487]. Por lo tanto, solo sirven las herramientas necesarias para que el cliente, bajo su cuenta y riesgo, realice las tareas oportunas de monitoreo. La herramienta AWS CLOUDTRAIL[488] de AMAZON, que puede integrarse en cualquier servicio de la nube de AWS AMAZON, permite a los clientes un monitoreo continuo y auditorías operativas de los datos, basado en un registro y almacenamiento automáticos de *logs* de actividades.

Para muchos proveedores puede ser de difícil aplicación las medidas anteriores, sin embargo, mejora el control de la nube para el cliente, con un coste mínimo para el prestador del servicio, incluir en los términos la notificación a los usuarios de los incidentes de seguridad[489]. Esta información es necesaria cuando, dentro del código de buenas prácticas del cliente, informa a los usuarios finales (por ejemplo, empleados de la entidad) de las medidas tomadas en materia de seguridad[490]. Estas medidas no suelen aparecer en los contratos estandarizados de la nube, argumentando su no inclusión por razones operativas. Sin embargo, notificar en un plazo razonable, máximo 24 horas desde que se producen los incidentes, o incluso comprometerse a hacerlo tan pronto como sea posible propicia que puedan ponerse en marcha medidas de seguridad en la organización, salvaguardando la información contenida. Un paso más sería establecer que sea directamente el cliente quien asuma la investigación de los incidentes acontecidos para determinar el cumplimiento de las medidas de seguridad establecidas por el proveedor, pudiendo conllevar, incluso, la rescisión del contrato. Sin embargo, esta medida estará

[487] Recoge, de manera expresa, que *"Microsoft Azure does not monitor for or respond to security incidents within the customer's area of responsibility*". SECURITY RESPONSE IN THE CLOUD de MICROSOFT AZURE, última actualización del proveedor 08.02.2017. Accesible en: https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678. Último acceso: 08.08.2018.

[488] Más información en la web de AWS CLOUDTRAIL, accesible en: https://aws.amazon.com/es/cloudtrail/. Último acceso: 08.08.2018.

[489] Esta notificación estimularía una acción correctiva por parte del cliente, generando confianza entre el sistema del proveedor utilizado en el entorno del *cloud* y otros sistemas, complementarios, que pueden integrarse en el servicio. Algunos informes que pueden cumplir dicho objetivo son:

- La información sobre los parches y controles establecidos frente a las vulnerabilidades detectadas.
- La información sobre los controles de compensación aplicados.
- Los datos sobre las vulnerabilidades y su tendencia, así como su clasificación y puntuación de gravedad (conforme al esquema de clasificación CVSS).

[490] INFORMATION COMMISSIONER'S OFFICE (ICO): "Guidance on the use of cloud computing: Data protection act 1998", 2012, v. 1.1., p.11.

lejos de acordarse ante proveedores de servicios *cloud* estandarizados y ante/para pequeños y medianos clientes.

MICROSOFT AZURE en el documento SECURITY RESPONSE IN THE CLOUD[491], ajeno al contrato del servicio, pero rector del proceder en el entorno de la nube, recoge ante los incidentes de seguridad que[492]:

"Cuando un incidente de seguridad es conocido, Microsoft establece un protocolo de notificación de incidentes para Azure, que incluye:

- *Notificación inmediata a los clientes afectados.*
- *En algunos supuestos, la notificación puede demorarse para cumplir la normativa aplicable, en este caso Microsoft se esforzará por tomar las precauciones que mitiguen el problema y minimicen el impacto.*
- *Notificación a las autoridades de regulación, si es requerida.*

Las notificaciones de los incidentes de seguridad se realizarán a los contactos establecidos en el centro de seguridad de Azure, pudiendo ser configurado siguiendo las pautas de implementación. De forma adicional, si no se proporciona la información de contacto en el centro de seguridad, la notificación se enviará al administrador o administradores del servicio del cliente. La notificación se llevará a cabo por el medio que Microsoft seleccione, incluido el email. Este medio es el considerado más oportuno para la mayoría de los incidentes. Proporciona una respuesta rápida a un gran número de clientes".

---

[491] SECURITY RESPONSE IN THE CLOUD de MICROSOFT AZURE, última actualización del proveedor 08.02.2017. Accesible en: https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678. Último acceso: 08.08.2018

[492] Traducción libre. Cita de origen: "*When a security incident is declared, Microsoft supports an incident notification process for Azure that includes:*

- *Prompt notification to affected customers*
- *In some instances, notification may be delayed at the direction of law enforcement, in which case Microsoft will endeavor to take precautions for the mitigation of the issue and minimize impact to our customers*
- *Notification to applicable regulatory authorities if required*

Notification of security incidents will be delivered to the listed security contacts provided in Azure Security center, which can be configured by following the implementation guidelines. Additionally, if contact information is not provided in Security Center, notification will be sent to one or more of a customer's administrators. Notification will be sent by any means Microsoft selects, including via email. Email is considered the most desirable approach for most issues. It provides the security response team great bandwidth to notify a lot of customers quickly".

Hay un cambio considerable en la política de MICROSOFT AZURE. Con anterioridad simplemente comunicaba a la entidad que tenía elaborado un plan de comunicación completo en el caso de incidencias, sin tener acceso a él los clientes antes de la contratación del servicio, ni estableciendo cuándo ni cómo se notificaría[493].

v. Lock-in y lock-out

La portabilidad de los datos y la conservación de los metadatos y los datos una vez finalizada la relación contractual, la dependencia excesiva a un proveedor de servicios o la portabilidad de las aplicaciones, muy importante en entornos *IaaS* y *PaaS*, resaltan la importancia de recoger en el clausulado del contrato aspectos relacionados con el *lock-in* y *lock-out* del servicio[494] [495].

Una de las principales preocupaciones de los usuarios es la conservación de los datos en un formato utilizable. Las razones pueden ser: en primer lugar, durante la relación contractual y terminada la misma, para cumplir con la normativa aplicable (por ejemplo, conservación de los últimos ejercicios fiscales), para litigios o por otras razones legales que le puedan afectar. Otra de las razones por la cual los clientes pueden requerir la

---

[493] Aunque se proporcionaba la información en español, facilitando a los clientes la comparativa entre proveedores, simplemente se recogía en el apartado de RESPUESTA A LOS INCIDENTES:
"En los servicios de la plataforma Windows Azure trabaja personal de operaciones las 24 horas del día, los 7 días de la semana. Si se produce un incidente de seguridad, el personal de operaciones implementará los procedimientos documentados que se deben seguir en ese caso. Asimismo, existe un plan de comunicación completo, que se implementará de igual forma en caso de producirse un incidente de seguridad".
Estaba accesible en: http://www.windowsazure.com/es-es/support/legal/security-overview/. Último acceso válido: 14.09.2013.

[494] ENISA propone una serie de cuestiones para entender los riesgos asociados a la vinculación con un proveedor de servicios en nube. A saber:

- ¿Existen procedimientos documentados y API para exportar datos desde la nube?
- ¿Ofrece el distribuidor formatos de exportación interoperables para todos los datos almacenados en la nube?
- En el caso del *SaaS*, ¿están normalizadas las interfaces API utilizadas?
- ¿Existen disposiciones para la exportación de aplicaciones creadas por el usuario en formato estándar?
- ¿Existen procesos para demostrar que los datos pueden exportarse a otro proveedor en la nube?
- ¿Puede realizar el cliente su propia extracción de datos para verificar que el formato es universal y puede migrar a otro proveedor en nube?

Extraído de ENISA: "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009, p. 87-88. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

[495] El estudio se centra en los datos no personales.

conservación de los datos una vez finalizada la relación contractual es la reutilización de datos para el posterior desarrollo de la actividad comercial. Por lo tanto, establecer contractualmente una herramienta de *e-discovery* durante el contrato y durante un periodo después de la finalización del mismo puede ser de gran utilidad.

DROPBOX[496] permite a las empresas, terminado el contrato, a petición del cliente y bajo el pago de un precio, el acceso a la cuenta para que pueda exportar los datos, eliminando los datos del sistema después de un "plazo comercial razonable"[497]. Genera la inseguridad de qué considera DROPBOX plazo razonable[498].

Más común, aunque menos garantista para el cliente, es la cláusula que reconoce a los usuarios la facultad de que le sean devueltos los datos en el *cloud* terminado el contrato. Aspectos para tener en cuenta deben ser la simplicidad del proceso, el formato de exportación de los datos, la asistencia del proveedor del servicio en la devolución de los datos (migración asistida) y el período de retención de los datos por el proveedor. Aunque puede ser habitual esta práctica en las nubes orientadas a las empresas, devolviendo los datos en un formato estándar (por ejemplo, CSV)[499], siempre es recomendable establecer compromisos contractuales, aunque impliquen un coste

[496] Se puede acceder DROPBOX BUSINESS AGREEMENT a través del siguiente enlace: https://www.dropbox.com/terms#business_agreement. Última actualización de las condiciones: 17.04.2018. Último acceso: 08.08.2018.

[497] Literalmente: *"If this Agreement terminates: (a) except as set forth in this Section, the rights and licenses granted by Dropbox to Customer will cease immediately; (b) Customer may, prior to termination, request reasonable additional time to export its Stored Data, provided that Dropbox may charge Customer for such extended access based on Dropbox's then-current standard fees; and (c) Dropbox will delete any End User Accounts and Stored Data relating to Customer's account in a commercially reasonable period of time following receipt of an Administrator's request to do so. Dropbox may make instructions available to Customer regarding how to submit the Administrator request described in clause (c) of the previous sentence".*

[498] La actualización del acuerdo ya supone un avance. En la revisión de 30.01.2017 no se recogía, de forma clara, la eliminación de los datos por el proveedor ("puede eliminar" los datos del sistema). Literalmente la clausula indicaba: *If this Agreement terminates: (a) except as set forth in this Section, the rights and licenses granted by Dropbox to Customer will cease immediately; (b) Dropbox may, at Customer's request, provide Customer access to its account at then-current fees so that Customer may export its Customer Data; and (c) after a commercially reasonable period of time, Dropbox may delete any Customer Data relating to Customer's account".*

[499] Tal es la importancia de esta medida que la cláusula 14 del *framework agreement* del UK G-Cloud, desarrollado en el Capítulo III.c.b, y extensible al resto de experiencias internacionales, establece que los formatos de transferencias de datos de los clientes deben ser en formato abierto o fácilmente convertible al formato requerido por el cliente, estableciendo la obligación a los proveedores de demostrar la capacidad de extracción de los datos si así se solicita.

adicional, sobre la devolución y la asistencia del proveedor en la devolución (migración asistida)[500].

En el supuesto de SAP CLOUD SERVICES[501], por ejemplo, el cliente *"puede exportar y recuperar sus Datos de Cliente en un formato estándar"*, lo que no quiere decir que sea abierto, estableciendo además que *"antes de que venza el Plazo de Suscripción, el Cliente puede utilizar las herramientas de exportación de autoservicio de SAP para realizar la exportación"*, por lo tanto, facilita al cliente la migración de los datos, e imposibilita al cliente exportar los datos terminado el contrato al eliminar *"los Datos de Cliente que permanezcan en los servidores alojados en el Servicio Cloud"*.

El período de recuperación de los datos una vez finalizado el contrato, y antes de ser eliminados completamente, es un aspecto a tratar en esta cláusula. En gran medida dependerá de los servicios demandados, y de las circunstancias de los clientes y datos (o aplicaciones) para migrar a otro proveedor de servicios. Es razonable que, si se contrata un servicio de migración, pudiendo incluso establecerse como contrato *outsourcing*, el plazo de eliminación de datos se prorrogue a un período más extenso terminada la relación contractual principal. Sí parece oportuno acordar contractualmente que se notifique a los clientes dicha operación antes de la eliminación completa.

En el contrato vigente de WINDOWS AZURE[502], dentro de su clausulado establece que es un *"contrato completo con respecto a su objeto y sustituye cualquier comunicación anterior o simultánea"*, no recoge ninguna cláusula referente a la devolución y eliminación de los datos del cliente, distinguiendo si el servicio es gratuito (la eliminación puede ser inmediata) o de pago[503].

---

[500] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 31-32.

[501] Se puede acceder a los TÉRMINOS Y CONDICIONES GENERALES PARA SAP CLOUD SERVICES en: https://assets.cdn.sap.com/agreements/general-terms-and-conditions/cls/general-terms-and-conditions-for-sap-cloud-services-direct-spain-spanish-v2-2017.pdf. Versión v.2-2017. Último acceso: 08.08.2018.

[502] Contrato de WINDOWS AZURE, versión de abril 2018. Accesible en: https://azure.microsoft.com/es-es/support/legal/subscription-agreement/. Último acceso: 08.08.2018.

[503] La versión de septiembre de 2013 dictaba: *"Puede extraer y/o eliminar Datos del Cliente en cualquier momento. Cuando una Suscripción expire o termine, conservaremos los Datos del Cliente que no haya eliminado por al menos 90 días, de modo que pueda extraerlos, salvo por las pruebas gratuitas, donde podemos eliminar inmediatamente los Datos del Cliente, sin período de retención. Usted seguirá siendo*

El poder recuperar los datos por el cliente debe estar ligado al proceso de eliminación de los datos innecesarios, no relevantes para el traslado del servicio entre proveedores o necesarios por requerimiento expreso. Es decir, además del período de dilación estudiado anteriormente para que podamos migrar los datos, debe establecerse si los datos serán eliminados de forma automática por el proveedor de servicios o debe el cliente solicitar la eliminación. En ocasiones, según las necesidades del contratante, es importante establecer el procedimiento a seguir no solo cuando se termina la relación contractual, sino cuando en el curso de la misma los clientes eliminan algunos datos que estaban en uso. Cuando se eliminan datos de la nube raramente son retirados de los medios de almacenamientos subyacentes, si no se toman algunas medidas adicionales. Además, es probable que el proveedor tenga múltiples copias de los datos almacenados en varias ubicaciones[504].La eliminación completa de los datos, incluido los datos que mantengan los sub-procesadores, es bastante compleja, dado que requiere sobreescribir un número mínimo de veces sobre los datos e incluso, como medida extrema e inequívoca, la destrucción segura de los medios de almacenamiento físicos. Dificultad que se agrava por la propia mecánica del *cloud*, que implica a diferentes equipos en la prestación del servicio con un constante flujo de datos. Por lo tanto, dado que requiere unos elevados costes económicos, el cliente debe valorar la importancia de los datos, el nivel de seguridad requerido y las aplicaciones que utiliza en la nube. Por ejemplo, si se utiliza un servicio *SaaS* que implica un procesamiento temporal de datos, las cláusulas de eliminación total pueden no ser muy relevantes al no permanecer de forma constante los datos. De este modo, no se acordará el método de eliminación de datos más seguro, destrucción física, por los problemas económicos y técnicos, salvo que sea estrictamente necesario.

responsable de los costos de almacenamiento y de otros costos aplicables durante este período de retención. Tras la expiración de este período de retención, eliminaremos todos los Datos del Cliente, incluida toda copia de seguridad o almacenada en caché, dentro de 30 días desde el término del período de retención. Usted acepta que no tenemos ninguna obligación adicional de conservar, exportar o devolver los Datos del Cliente y que la eliminación de sus Datos del Cliente, conforme a estos términos, no conlleva ningún tipo de responsabilidad por nuestra parte."

[504] INFORMATION COMMISSIONER'S OFFICE (ICO): "Guidance on the use of cloud computing: Data protection act 1998", 2012, v. 1.1., p. 16-17.

La herramienta G SUITE[505] para empresas de GOOGLE recoge entre los efectos de cancelación de datos *"…iii) tras un periodo de tiempo comercialmente razonable, Google eliminará los Datos de cliente mediante la supresión de redireccionamientos que hagan referencia a estos en los servidores activos y de replicación de Google y sobrescribiéndolos conforme transcurra el tiempo, iv) cada una de las partes aplicará de inmediato todos los esfuerzos comercialmente razonables para devolver o destruir cualquier otra Información confidencial de la otra parte, si así se solicita"*. Sin embargo, no establece el plazo en el que se eliminarán los archivos ni los procesos concretos de eliminación, solo el "redireccionamiento". DOCUMENT CLOUD[506] de ADOBE faculta al cliente la transición de los datos, si bien, indica que *"debe completarse en un plazo de 30 días desde la terminación o vencimiento de su licencia para el servicio de firma electrónica. Al final de este período de transición de 30 días, Adobe se reserva el derecho de eliminar cualquier Dato del cliente"*. Por lo tanto, se positiva no como un derecho del cliente de garantizar que los datos alojados en la nube sean inutilizables o eliminados, sino como una facultad del proveedor para no facilitar al cliente la migración.

vi. Derechos de Propiedad Intelectual e Industrial

Cláusula común en todos los contratos informáticos, tratada dentro del marco general de la contratación, debe estudiarse de manera singular cuando el servicio se circunscribe a la contratación en la nube. De forma general podemos indicar que en la citada disposición se discute sobre la titularidad de los derechos de propiedad intelectual e industrial, fundamentales en los contratos de *cloud* debido a que para el correcto desarrollo del servicio objeto del contrato son necesarios medios protegidos por los derechos de referencia[507]. Anteriormente hemos tratado la responsabilidad del cliente y del proveedor por las infracciones de los derechos de propiedad. DÁVARA RODRÍGUEZ[508] recuerda que la transmisión de cualquier derecho, entre los que se

[505] ACUERDO DE G SUITE, a través de distribuidor, versión 08.08.2018. Accesible en: https://gsuite.google.com/intl/es/terms/reseller_premier_terms_ie_es.html. Último acceso: 08.08.2018.

[506] CONDICIONES ADICIONALES DE USO de DOCUMENT CLOUD, versión 16.06.2016. Accesible en: http://www.adobe.com/content/dam/acom/es/legal/servicetou/Document-Cloud_Additional_TOU-es_ES_20160616.pdf. Último acceso: 08.08.2018.

[507] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 73.

[508] DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, Thomson-Aranzadi, 2008, p. 297.

incluyen la propiedad intelectual e industrial, de los existentes en un contrato informático deberá quedar sometido, mediante acuerdo contractual, al consentimiento de la otra parte. De esta forma, salvo que exista consentimiento expreso y escrito, ninguna de las partes podrá ceder los derechos de propiedad intelectual e industrial del contrato a ninguna otra persona, de ninguna forma. Por este sentido, deben quedar claros los derechos que corresponden conjunta e individualmente a las partes del contrato al perfeccionarse.

Partiendo de esta premisa, se debe consensuar con los proveedores de la nube a quién le corresponde la propiedad de los datos procesados en el entorno. Especialmente relevante puede ser en la modalidad *IaaS* o *PaaS*, dado que son los usuarios (clientes) quienes desarrollan o implementan las aplicaciones que sirven de base al modelo. En la prestación del servicio a veces es difícil discernir de manera clara cuándo la aplicación es desarrollada por el cliente y cuándo se sirve de herramientas establecidas o integradas por el proveedor de servicios[509]. Esta delimitación se hace más complicada cuando el cliente contrata los servicios de *cloud* mediante un integrador (intermediario), que puede desarrollar aplicaciones para sus propios clientes.

La herramienta G SUITE[510] de GOOGLE deja claro que los derechos de propiedad intelectual aportados por el cliente en el desarrollo del servicio son de su pertenencia, al establecer que *"excepto en lo establecido de forma expresa en este documento, este Acuerdo no garantiza a ninguna de las partes ningún derecho, implícito o no, al contenido o a cualquier parte de la propiedad intelectual del otro. Tal como establecen las partes, el Cliente posee todos los Derechos de propiedad intelectual de los Datos de cliente, y Google posee todos los Derechos de propiedad intelectual de los Servicios"*. Términos más oscuros plantea RED HAT OPENSHIFT, que permite el uso de la nube bajo la configuración *PaaS*, en su SERVICES AGREEMENT[511] al recoger: *"You agree that Red Hat and its licensors own all legal rights and interests, including intellectual property rights, in the Services. As part of the Services, You may receive access to certain*

[509] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 38-39.

[510] ACUERDO DE G SUITE, a través de distribuidor, versión 08.08.2018. Accesible en: https://gsuite.google.com/intl/es/terms/reseller_premier_terms_ie_es.html. Último acceso: 08.08.2018.

[511] ONLINE SERVICES AGREEMENT de RED HAT OPENSHIFT, versión de 02.05.017. Accesible en: https://www.openshift.com/legal/terms.html. Último acceso: 08.08.2018.

Software…, … You only acquire the right to use the Services and do not acquire any rights of ownership in the Services…, … Red Hat reserves all rights to the Services not expressly granted herein..".

Es fundamental reconocer los derechos que recaen sobre las partes en el contrato o en sus anexos, así como el uso y la autorización por el titular del derecho que con motivo de la materialización del servicio hicieren las partes. IWORD.COM[512] de APPLE reconoce que *"a excepción del material para el que le concedemos licencia, Apple no reclama la propiedad de los materiales ni del Contenido que envíe o ponga a disposición a través del Servicio"*, sin embargo, establece que *"si envía o publica dicho Contenido en áreas del Servicio accesibles al público, usted concede a Apple una licencia de uso mundial, libre de regalías y no exclusiva para usar, distribuir, reproducir, modificar, adaptar, publicar, traducir, comunicar públicamente y exhibir públicamente dicho Contenido a través del Servicio exclusivamente con el fin para el que se envió o se puso a disposición el Contenido"*.

Dos aspectos más se relacionan con los citados derechos y el entorno en la nube. En primer lugar, debe conocerse a quién corresponden los derechos de propiedad que surgen de las mejoras derivadas de las sugerencias o experiencias de los clientes. En este caso, puede ser oportuno requerir, al menos, el consentimiento del cliente si se quiere trasladar dichas mejoras a otros usuarios del proveedor. Y, en segundo lugar, algunas aplicaciones utilizadas por los clientes de la nube pueden estar protegidas por licencias. Por lo tanto, el clausulado debe aclarar si el servicio ofrecido por el proveedor cubre el uso de las aplicaciones. De igual forma, si se instalan aplicaciones de terceros (común en el entorno *IaaS* y *PaaS*), serán los usuarios quienes deban tener derecho de uso sobre las licencias. Puede ser oportuno, en este caso, determinar contractualmente si el cliente puede cargar aplicaciones de terceros y si el proveedor puede utilizar las aplicaciones instaladas por el cliente. GARCÍA DEL POYO[513] resume este considerando en "*la importancia de que cada una de las partes se asegure de que la otra acepta mantenerla indemne respecto de*

[512] PUBLIC BETA CONDICIONES DE SERVICIOS de IWORD.COM, revisión de 19.01.2010. Accesible en: https://www.apple.com/legal/iworkcom/es/terms.html. Último acceso: 08.08.2018.

[513] GARCÍA DEL POYO, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012, p. 73.

cualquier reclamación de un tercero derivada de un uso no autorizado de elementos protegidos por derechos de propiedad intelectual e industrial".

El beneficiario de los servicios de *cloud* siempre tendrá un licenciamiento de uso, por lo que será necesaria la autorización del titular de los derechos o licenciante si se realiza un comportamiento distinto del indicado.

vii. Acuerdo de Nivel de Servicios (ANS o SLA)

Frecuentemente establecido en un anexo al contrato principal de la computación en la nube, la referencia a los Acuerdos de Nivel de Servicios, con acrónimo ANS o SLA, es obligatoria por cuanto incide de manera directa en la mayoría de las cláusulas del contrato en la nube. Los ANS establecen una serie de indicadores o condicionantes técnicos que regulan el devenir del servicio, para que se mantenga en unas condiciones óptimas de prestación, determinará si el objeto del contrato se cumple y la responsabilidad por las caídas del servicio o el funcionamiento anormal, entre otros aspectos.

La definición más certera sobre qué es y en qué consiste un Acuerdo de Nivel de Servicios es dada por JANSEN y GRANCE:

"An SLA represents the understanding between the cloud consumer[514] *and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud consumer. The privacy policy documents information handling practices and the way consumer information is collected, used, and managed by the cloud provider, while the acceptable use policy identifies prohibited behaviours by cloud consumers. The terms of use cover other important details such as licensing of services, limitations on liability, and modifications to the terms of the agreement. Privacy and security risks depend to a great extent on the terms established in the service agreement"*[515][516].

---

[514] *Consumer* entendido como clientes, es decir, tanto para las relaciones B2C como B2B.

[515] JANSEN, Wayne y GRANCE, Timothy: "Guidelines on Security and Privacy in Public Cloud Computing", *National Institute of Standards and Technology, US. Department of Commerce*, 2011, p. 17-18. Accesible en: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Último acceso: 08.08.2018.

[516] Traducción libre: *"Un ANS (SLA) representa el entendimiento entre el consumidor de la nube* (entendido de manera amplia) *y el proveedor sobre el nivel de servicios esperados en el servicio y, en el caso de que el proveedor no se adecúe al nivel acordado, la compensación disponible para el consumidor en la nube. La política de privacidad documenta las prácticas de tratamiento de la información y la forma en que la*

De esta forma, el ANS viene a recoger una serie de parámetros objetivos establecidos entre el demandante del servicio y el proveedor, donde se concreta el cumplimiento del servicio, así como el modo de proceder cuando surgen problemas de carácter técnico, el tiempo de reacción ante los mismos, la disponibilidad del servicio y los niveles máximos o mínimos de disponibilidad de determinados valores[517]. Como complemento, debe ser un documento debidamente detallado, buscando la mayor objetividad posible, con el fin de determinar claramente en caso de incumplimiento[518]. Debe ser lo suficientemente claro para evitar discrepancias en las interpretaciones. Este nivel de detalle ha propiciado que en muchos ANS se recojan cláusulas de revisión de parámetros y de cuantificación establecidas, al surgir necesidades imprevistas con el desarrollo del servicio.

Decíamos en capítulos anteriores que la complejidad del *cloud*, uno de sus rasgos definitorios respecto a otros contratos informáticos, es la combinación de obligaciones de resultados con obligaciones de medios. Precisamente los objetivos de nivel de servicio suponen un criterio de medición del grado de cumplimiento del proveedor. Un desarrollo inferior al acordado podría ser causa de resolución del contrato por incumplimiento[519].

Parece lógico que ante grandes demandas de servicios de *cloud*, los clientes intenten debatir los métodos para medir los niveles de servicios adecuados. Los clientes podrían requerir numerosos indicadores claves de rendiento. Sin embargo, en el estudio realizado por HON, MILLARD y WALDEN se refleja que la mayoría de los proveedores de servicios de computación en la nube se niegan a negociar con los clientes los niveles de

---

información del consumidor es recopilada, utilizada y administrada por el proveedor de la nube, mientras que la política de uso aceptable identifica los comportamientos prohibidos por el consumidor. Los términos de uso determinan otros aspectos importantes como la concesión de licencias, las limitaciones de responsabilidad y las modificaciones de los términos del acuerdo. Los riesgos y la seguridad asociada a la privacidad dependen en gran medida de los términos establecidos en el acuerdo (contrato) *del servicio".*

[517] GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing". *Derecho y cloud computing*, 2012, p. 198.

[518] Sirva de ejemplo el proveedor MICROSOFT. Establece, de forma independiente, un "Contrato de Nivel de Servicio para Servicios Online de Microsoft". Accesible en: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=12528 (versión española de 01.07.2017). Último acceso: 08.08.2018.

[519] En el próximo apartado hablaremos de la extinción del contrato de la nube.

servicios, justificando esta medida sobre la base de que proporcionan servicios de consumo masivo[520].

El ETSI[521] resalta que el ANS es un documento determinante en las tres fases del ciclo de vida de la nube:

- En el anuncio de oferta y en la adquisición del servicio, permite al cliente valorar las opciones del mercado en función de sus necesidades.
- En el desarrollo del servicio, para determinar si se cumplen los niveles de servicios definidos y tomar las medidas correctivas, en caso de incumplimiento.
- Terminado el contrato, como instrumento para valorar la adecuación del servicio y sus posibles consecuencias. Además, puede determinar qué sucede con los datos.

Por lo expuesto, se requiere que el ANS esté bien definido, esté determinado, se correlacionen los objetivos de nivel de servicio con el servicio a recibir por el cliente, y sean comparables con otros proveedores.

Determinar de forma correcta el nivel de servicios adecuado es crítico y complejo. Si consideramos que el servicio de *cloud* debe tener como principales características la disponibilidad, fiabilidad del servicio y el rendimiento, unido a determinadas aplicaciones de misión crítica y servicios en tiempo real, la medición de tales niveles constantemente podría ocasionar una sobrecarga en las infraestructuras de los proveedores que puede redundar en el rendimiento de las aplicaciones utilizadas por los distintos usuarios del proveedor. Por este motivo, muchos de los proveedores garantizan el rendimiento de las aplicaciones respecto a un máximo de usuarios en línea. Otros aspectos por determinar pueden ser cómo y cuánto tiempo se tardará en restaurar una copia de seguridad en el supuesto en el que los sistemas se apaguen o los datos se pierdan, y si los proveedores tienen la responsabilidad de notificar previamente a los clientes las modificaciones en los estándares establecidos (que normalmente se publican en la web del proveedor) o

[520] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 14-15.

[521] ETSI: "Cloud Standards Coordination - Final Report", 2013, November, version 1.0, p. 6-7. Accesible en: https://ec.europa.eu/digital-single-market/en/news/cloud-standards-coordination-final-report. Último acceso: 08.08.2018.

corresponde a los usuarios monitorear los *websites* de los proveedores para determinar los posibles cambios[522].

Aunque pueden aparecer como cláusulas contractuales tipo diferenciadas, los Acuerdos de Nivel de Servicio referencian la forma de garantizar la integridad de los datos, la capacidad de recuperación y la continuidad del servicio. Estas medidas intentan salvaguardar la continuidad del negocio y la recuperación de los datos. Por ello, los clientes deberían discriminar entre los proveedores de servicio que garantizan copias de seguridad de los datos, y lo que es más relevante, si se comprometen y responsabilizan contractualmente a la realización de las copias; si establecen un sistema de garantías de integridad de los datos; y si asumen las pérdidas ante supuestos de no recuperación. Debe advertirse que esta cláusula no encuentra similitud, en cuanto a la finalidad, a las disposiciones referentes a la confidencialidad de los datos suministrados o de acceso no autorizado a los datos del usuario, dado que la responsabilidad por falta de confidencialidad cubriría la violación en la seguridad de los datos, pero no la pérdida o corrupción de estos. La determinación de la responsabilidad en este ámbito dependerá del servicio de *cloud* requerido, como hemos valorado a la hora de determinar las cláusulas de responsabilidad. Los usuarios tienen más control sobre la integridad de los datos, las copias y la seguridad en los modelos *IaaS* y *PaaS*, dado que en los modelos *SaaS* se utilizan aplicaciones estandarizadas proporcionadas por el proveedor de servicios.

AMAZON WEB SERVICES[523] señala, antes de recoger de forma definida la responsabilidad de cada una de las partes, que, antes de entrar en los detalles de cómo AMAZON asegura los servicios requeridos, la responsabilidad de la seguridad en la nube es compartida entre el cliente y el proveedor, siendo el prestador del servicio responsable de asegurar la infraestructura que soporta la nube y el cliente de los datos traslados y la

[522] Los cambios en el servicio serán tratados en el siguiente apartado.

[523] OVERVIEW OF SECURITY PROCESSES de AMAZON WEB SERVICES (AWS), versión de mayo de 2017. Accesible en: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf. Último acceso: 08.08.2018.

conexión al *cloud*[524][525]. MICROSOFT[526] se pronuncia en similares términos al establecer que *"usa un modelo de administración de riesgos basado en la responsabilidad compartida con el cliente: Microsoft es responsable de la plataforma, incluidos los servicios que ofrece, e intenta prestar un servicio en la nube que pueda cubrir las necesidades de seguridad, privacidad y cumplimiento de su organización. Como cliente, usted es el responsable del entorno una vez que se ha proporcionado el servicio. Debe identificar cuáles son los controles que se aplican a su empresa, y comprender cómo implementarlos y configurarlos para poder administrar la seguridad conforme a los requisitos normativos pertinentes".* Esta política de responsabilidad compartida también se traslada a la protección de datos[527].

El ANS debería contener las penalizaciones al proveedor de servicios ante el incumplimiento de las disposiciones establecidas. Lo habitual es que el régimen de responsabilidad derive en medidas de carácter económico, si bien las fórmulas son bastantes complejas. Suelen utilizar un parámetro común: un importe económico tomado como referencia relacionado con la desviación producida entre el valor objetivo establecido en el Acuerdo de Nivel de Servicios y el nivel de servicios realmente ofrecido.

---

[524] De forma literal establece: *"Before we go into the details of how AWS secures its resources, we should talk about how security in the cloud is slightly different than security in your onpremises data centers. When you move computer systems and data to the cloud, security responsibilities become shared between you and your cloud service provider. In this case, AWS is responsible for securing the underlying infrastructure that supports the cloud, and you're responsible for anything you put on the cloud or connect to the cloud. This shared security responsibility model can reduce your operational burden in many ways, and in some cases may even improve your default security posture without additional action on your part".*

[525] Más clara resultaba la versión de septiembre de 2013, no solo por su traducción al español: *"Usted construye sistemas encima de la infraestructura de nube de AWS. Por este motivo, las responsabilidades de seguridad son compartidas; AWS gestiona la infraestructura subyacente, pero usted tiene que asegurar todo lo que ponga en esa infraestructura. Esto incluye sus instancias de AWS EC2 y cualquier cosa que instale en ellas, todas las cuentas que tengan acceso a sus instancias, el grupo de seguridad que permita el acceso externo a sus instancias, la subred VPC en la que se alojan las instancias (si ha elegido esta opción), el acceso externo a sus depósitos de S3, etcétera.*
Esto significa que usted necesita tomar varias decisiones en torno a la seguridad, así como configurar varios controles. Si desea información para configurar un determinado servicio de AWS, consulte la documentación correspondiente a dicho servicio. Si desea más consejos relativos a las prácticas recomendadas en el ámbito de la seguridad, visite nuestra página de recursos de seguridad."

Estaba accesible en: http://aws.amazon.com/es/security/ (reseñas en español). Último acceso: 14.09.2013.

[526] MICROSOFT TRUST CENTER para los servicios en nube, versión 07.2017. Accesible en: https://www.microsoft.com/es-xl/trustcenter/guidance/risk-assessment. Último acceso: 08.08.2018.

[527] Véase: https://www.microsoft.com/es-xl/trustcenter/guidance/protect-data. Último acceso: 08.08.2018.

A pesar de estas penalidades económicas, muchos proveedores de *cloud computing* ante un incumplimiento del Acuerdo de Nivel de Servicios excluyen cualquier penalidad que no sean créditos en el servicio[528], incluso cuando no se presta el servicio en su totalidad, permitiendo la terminación opcional si los servicios realmente ofrecidos se encuentran por debajo de determinados porcentajes, establecidos en el propio documento del ANS. Solo en los supuestos de terminación de la relación del servicio parecen aceptar la responsabilidad y derivar alguna compensación monetaria. Aun así, el estándar de cláusulas limita el resarcimiento ante este incumplimiento, al exigir al usuario solicitar los créditos del servicio o las compensaciones económicas en un plazo predeterminado por el proveedor[529]. Es más, el empleo de cláusulas que limitan la responsabilidad a la cantidad total pagada por el cliente, a una cantidad que varía según el servicio contratado o incluso la negación total de responsabilidad en los servicios gratuitos es común entre los grandes proveedores de servicios de computación en la nube[530].

El servicio gratuito CLOUD DRIVE[531], como ejemplo a lo expuesto, excluye cualquier tipo de responsabilidad ante el cliente o cualquier tercero, incluso por problemas de conexión, acceso, uso o incapacidad de acceder o usar el sitio, contenidos, archivos y/o servicios[532].

---

[528] Uno de los proveedores que desarrolla de manera más detallada los créditos de servicios y las limitaciones al mismo es RACKSPACE en su CLOUD SLA, versión 13.08.2018. Accesible en: https://www.rackspace.com/information/legal/cloud/sla. Último acceso: 13.08.2018.

[529] HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117, p. 14-15.

[530] Por la similitud en el tratamiento por parte del proveedor del servicio, se recomienda recordar el estudio de las cláusulas de responsabilidad del Capítulo V.a.b.i.

[531] TERM OF SERVICE de CLOUD DRIVE, versión revisada el 08.08.2018. Accesible en: https://www.driveoncloud.com/term.html. Último acceso: 08.08.2018.

[532] De forma literal: *"In no event will cloud drive be liable to you or to any third party for damages of any kind, including, without limitation, direct, special, incidental, punitive or consequential damages (including loss of use, data, business or profits) arising out of or in connection with this agreement, or from your access to or use of, or inability to access or use, the site, content, files and/or services, or for any error or defect in the site, content, files or services, whether such liability arises from any claim based upon contract, warranty, tort (including negligence), strict liability or otherwise, or any other legal theory, whether or not cloud drive has been informed of the possibility of such damage, even if a remedy set forth herein is found to have failed of its essential purpose"*.

VELNEO[533], aunque en su documento público de ANS no recoge parámetros medibles por el cliente, establece que *"si se produce una interrupción en un mes natural superior a 25.920 segundos, Velneo descontará en la siguiente factura de los servicios de Velneo Cloud un 4 % de la base imponible cobrada al cliente por el servicio por cada hora de interrupción adicional del servicio, hasta un 100% de la base de cuota mensual recurrente correspondiente a los servicios de Velneo Cloud"*, limitando la capacidad de resarcirse de los daños producidos a un porcentaje máximo y solo en créditos del servicio (aunque en este caso sea contra factura). MICROSOFT[534] limita la posibilidad de crédito a una *"reclamación dentro de los dos (2) meses posteriores a la finalización del mes de facturación en que tuvo lugar el Incidente objeto de la reclamación"*.

viii. Cambio de las características del servicio y renovación del ANS

Los contratos que tienen como objeto el desarrollo de servicios relacionados con las nuevas tecnologías deben ser lo suficientemente flexibles para adaptarse a la evolución y a las mejoras técnicas. La computación en la nube no es un supuesto aislado, si bien, debe estudiarse con detenimiento quién ostenta las facultades de modificación del contrato y a qué obedece el cambio. Del análisis de los contratos estándares de la nube se extrae que el proveedor tiene la facultad de cambiar las condiciones contractuales unilateralmente. Por consiguiente, el cliente deberá, en primer lugar, atender de la existencia o no de una cláusula contractual que permita la modificación unilateral por el proveedor del servicio y, en segundo lugar, si antes de producirse la modificación, el cliente posee el derecho a ser notificado de cualquier cambio y puede ejercer, ante su disconformidad, la facultad de rescindir la relación contractual sin penalización. La incorporación de este derecho equilibra la relación de fuerza entre las partes.

---

[533] SLA público de VELNEO, revisado el 08.08.2018. Accesible en: https://doc.velneo.es/sla.html. Último acceso: 08.08.2018. En la versión anterior, que estaba accesible en https://velneo.es/sla-velneo-cloud/, se recogían parámetros objetivos de acceso público antes de contratar el servicio.

[534] CONTRATO DE NIVEL DE SERVICIO PARA SERVICIOS ONLINE de MICROSOFT, versión de 01.07.2017. Accesible en: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=12528. Último acceso: 08.08.2018.

AWS[535] de AMAZON, por ejemplo, se reserva el derecho a cualquier cambio, trasladando al cliente la carga de revisar los términos y políticas que regirán el servicio (*"please review our other policies on the AWS Site. These policies also govern your visit to the AWS Site. We reserve the right to make changes to the AWS Site, policies, and these Site Terms at any time"*). ARSYS[536] también establece la facultad de modificar unilateralmente las características y condiciones del servicio de computación en la nube, si bien *"deberá cumplir más formalidad que la de informar al cliente con un aviso on-line y/o llevar esta modificación a las cláusulas de las Condiciones contractuales que le sean de aplicación y/o remitirlo por correo electrónico"*, sin perjuicio de comunicar al cliente *"por escrito estas modificaciones en el menor tiempo posible para su adaptación por el cliente"*. Añade la posibilidad de resolver por el cliente las condiciones generales de contratación o las condiciones específicas del contrato de la nube afectadas en el plazo de *"14 días naturales desde que recibe dicha comunicación"*. UKFAST[537], a pesar de reconocer que la compañía notificará al cliente cualquier cambio significante en las condiciones del servicio, no establece cómo realizará la comunicación ni dónde puede encontrar las últimas condiciones del servicio actualizadas[538].

Esta facultad de cambio en las condiciones que el proveedor se atribuye tiene mayor o menor significado dependiendo del servicio en la nube que se requiera, así como de la cantidad y de la calidad de información suministrada. Cuando el modelo empleado es *IaaS* o *PaaS*, un cambio en el proveedor de servicios puede hacer necesario reescribir el código de la aplicación para integrarse con las API del proveedor. En este sentido, cuando los servicios en la nube son elevados, los clientes pueden tener la necesidad de garantizar que no se producirán cambios en el servicio, aunque sean mínimos o de menor

[535] SITE TERMS de AWS, última versión: 23.12.2011. Accesible en: https://aws.amazon.com/es/terms/. Último acceso: 08.08.2018.

[536] CONDICIONES GENERALES DE SERVICIO de ARSYS. Accesible en: https://www.arsys.es/legal?dhtml=condiciones-generales-contratacion. Condiciones a fecha de 08.08.2018 (CGS_23052018). Último acceso: 08.08.2018.

[537] TERMS AND CONDITIONS de UKFAST, versión 07.2017. Accesible en: https://www.ukfast.co.uk/terms/terms-and-conditions.html#setupoption. Último acceso: 08.08.2018.

[538] De forma literal establece: *"The Company reserves the right to vary the Conditions as a result of changes required by its insurers, for operational or administrative reasons or in order to comply with changes in the law. 28.2 The Company will provide the Customer with 14 days' notice of any significant changes to the Conditions"*.

importancia, sin su conocimiento. En grandes clientes de *cloud* es recomendable exigir contractualmente que se notifiquen los cambios clave del servicio, así como su impacto. Con un preaviso, pueden evaluar los cambios que va a realizar el proveedor, los perjuicios que puede tener en el desarrollo de su actividad, iniciar conversaciones con otros proveedores del servicio y decidirse, si así lo tiene establecido, a resolver el contrato. Debemos resaltar, como identifican BRADSHAW, MILLARD y WALDEN, que la cláusula de rescisión por la que el cliente puede no aceptar la modificación de los términos del contrato se recoge habitualmente en los servicios no gratuitos de grandes clientes[539].

c. Epítome sobre la extinción del contrato de computación en la nube entre empresas: causas y efectos de las obligaciones.

En el subapartado de las condiciones generales de contratación, en duración y terminación del contrato, y en el subapartado relativo a las cláusulas específicas del contrato, *lock-in* y *lock-out*, se ha tratado de forma tangencial las causas y efectos terminado el contrato de la computación en la nube. A menudo, se le presta escasa atención a qué sucederá con nuestros datos extinta la relación contractual y las implicaciones que puede tener para los clientes la finalización del servicio de la nube, a nivel operativo y obligacional. Este epítome intenta condensar las principales causas y efectos de la extinción contractual en las relaciones B2B.

Entre las causas de extinción del contrato de computación en la nube están el desistimiento unilateral de una de las partes, la resolución por incumplimiento o la imposibilidad sobrevenida para la prestación del servicio.

La diferente posición contractual del cliente y el prestador de servicios es manifiesta ante el desistimiento unilateral de las partes. Mientras que es común que al cliente se le penalice su intención de extinguir la relación contractual, aun mediando un plazo razonable en la comunicación, el proveedor suele reservarse el derecho a cancelar el servicio sin preaviso. En el servicio AMAZON DRIVE[540], el proveedor se reserva la potestad de *"resolver el Contrato o restringir, suspender o resolver el uso por parte de*

[539] BRADSHAW, Simon; MILLARD, Christopher y WALDEN, Ian: "Contracts for Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", *Queen Mary University of London - Legal Studies Research Paper*, 2010, nº 63, p. 21.

[540] CONDICIONES DE USO de AMAZON DRIVE, modificación del 09.06.2018. Accesible en: https://www.amazon.es/gp/help/customer/display.html?nodeId=201376540. Último acceso: 08.08.2018.

usted del Servicio a nuestra entera discreción en cualquier momento". Sin embargo, para el servicio AWS[541] el cliente y el proveedor pueden dar por terminado el contrato por cualquier razón, informando al respecto a la otra parte y cerrando todos los servicios activos con las herramientas que dispone, en caso de elección del cliente, el proveedor de servicios. Solo señala plazo expreso cuando la terminación del contrato es dispuesta por AMAZON: *"nosotros podremos terminar este Contrato por cualquier razón mediante aviso con un mínimo de 30 días de anticipación"*. Resulta paradójico que una entidad tenga diferente regulación en la terminación del contrato, que en principio no requieren unos servicios o requerimientos materiales especializados, en función del público objetivo y la finalidad de la nube.

Frente al desistimiento unilateral, se encuentra la resolución del contrato por el incumplimiento de una de las partes. La protección en las obligaciones sinalagmáticas que brinda nuestro ordenamiento jurídico ante el incumplimiento de los sujetos parte de la regulación establecida en el artículo 1.124 del CC. El sujeto que ha cumplido la obligación contractual tiene la potestad de instar al cumplimiento o la resolución de las obligaciones con el resarcimiento de daños y perjuicios en ambos casos. En palabras de MONTÉS PENADÉS[542], el *ius variandi*, que permite pedir la resolución contractual, incluso después de haber compelido el cumplimiento cuando resultare imposible, precisa que sea un incumplimiento resolutorio, es decir, sea de una gravedad tal que impida la verdadera ejecución del contrato por no satisfacer el interés de la parte. Se ha analizado que, en el contrato de la computación en la nube, la no prestación de un servicio que satisfaga las necesidades del cliente de manera reiterada, por una parte, o el incumplimiento del pago del servicio o la política de usos del servicio, por otra, se configuran como obligaciones esenciales. Esto no impide, ante incumplimientos parciales, la resolución del contrato siempre que tales incumplimientos sean significativos y afecten a las obligaciones principales de las partes[543]. Por lo tanto, será esencial determinar cómo afecta la deficiente prestación del servicio por el proveedor, la falta de

[541] Se puede acceder al CUSTOMER AGREEMENT de AWS a través del siguiente enlace: https://aws.amazon.com/es/agreement/. Condiciones a fecha de 08.08.2018 (Última modificación: 01.07.2018). Último acceso: 08.08.2018.

[542] MONTÉS PENADÉS, Vicente: "La Defensa del Derecho de Crédito", *Derecho Civil – Derecho de obligaciones y contratos*, 2001, Tirant lo Blanch, p. 164-165.

[543] DIEZ-PICAZO, Luis: "La protección del Derecho de crédito lesionado y las relaciones obligatorias sinalagmáticas", *Fundamentos del Derecho Civil Patrimonial. Volumen II: las relaciones obligatorias*, 2007, Thomson, p. 830.

acceso, las interrupciones del servicio o las alteraciones en la nube contratada para dictaminar si imposibilitan cumplir el objetivo que se persigue con la contratación o si entran en juego otros mecanismos de compensación ante un cumplimiento deficiente. El impago del cliente devendrá esencial cuando sea reiterado o, ante el requerimiento del proveedor, desoiga la petición y no satisfaga el importe económico.

Aunque olvidado en los supuestos de extinción de obligaciones, como recalca ORDUÑA MORENO[544], artículo 1.156 del CC, la imposibilidad sobrevenida de la prestación, extingue la relación obligatoria. Su alcance depende de la no imputabilidad a alguna de las partes del hecho que imposibilita la prestación del servicio, siendo *"representativa de un hecho o circunstancia que obsta el normal desenvolvimiento del deber de prestación, bien determinando la imposibilidad de su correspondiente ejecución, bien mermando significativamente el valor o la utilidad de la misma para el acreedor"*[545]. El problema, como hemos dejado de manifiesto en nuestro estudio, reside en la desigual distribución de la responsabilidad y los riesgos en la relación manifestados en los términos y condiciones contractuales, notorios, en este caso, en la asunción por el cliente de las consecuencias de los hechos que impiden la ejecución. Se ha citado, en el estudio de la responsabilidad, las condiciones de GOGRID, ACENS o CREATOR de ZOHO. Es esencial el estudio de la cláusula contractual porque, además de las exenciones de responsabilidad del prestador del servicio, son habituales cargas adicionales al cliente[546].

Esta introducción sobre las causas de extinción de la relación contractual de la nube, nos permite evaluar los efectos que se producen cancelada o finalizada la prestación principal, conocida como la "reversibilidad" del *cloud computing*.

---

[544] ORDUÑA MORENO, Javier: "Extinción de la obligación", *Derecho Civil – Derecho de obligaciones y contratos*, 2001, Tirant lo Blanch, p. 208.

[545] ORDUÑA MORENO, Javier: "Extinción de la obligación", *Derecho Civil – Derecho de obligaciones y contratos*, 2001, Tirant lo Blanch, p. 209.

[546] Siguiendo nuestro ejemplo, ACENS establece que *"la causa fortuita o los eventos de fuerza mayor, así como la terminación de las Condiciones de Contratación fundamentada en las anteriores, no exonerará al Cliente del cumplimiento de las obligaciones de pago pendientes hasta la fecha de interrupción de los Servicios"*. CONDICIONES GENERALES DE CONTRATACIÓN ELECTRÓNICA Y TELEFÓNICA DE SERVICIOS ACENS, vigente el 08.08.2018. Accesible en: https://www.acens.com/file_download/condiciones_generales_de_contratacion_electronica_acens.pdf. Último acceso: 08.08.2018.

Se ha expuesto dentro de las cláusulas generales que rigen el contrato de la computación en la nube que, aunque el cliente en términos jurídicos no tiene una facultad esencial de recuperación de los datos e información trasladada, se han desarrollado teorías jurídicas que, sobre la base del principio de buena fe y por analogía con el contrato de arrendamiento, se afirma que el contratante ostenta la facultad de recuperación. Recuperación y portabilidad no son conceptos sinónimos, si bien, no se entienden de forma aislada porque el cliente que recupera los datos e información en la nube previsiblemente tenga la necesidad de portarlos a otro proveedor de servicio o, en el menor de los casos, a otra herramienta informática. Por otra parte, la portabilidad no está circunscrita solo a los datos e información en la nube, en función del tipo y modo de despliegue de la nube, el cliente puede integrar aplicaciones en los servicios del proveedor, lo que vuelve a refrendar la necesidad de utilizar formatos utilizables, principalmente estándares y en abierto.

El Anteproyecto de Código Mercantil establece entre las obligaciones principales del prestador del servicio, en el contrato de alojamiento, posibilitar la recuperación de la información almacenada por el cliente[547]. ROSSELLÓ RUBERT[548] argumenta el derecho de recuperación de los datos del cliente, ante la inexistente regulación jurídica, en la obligación del proveedor de guardar y restituir la cosa, por aplicación analógica del régimen dispuesto para el contrato de depósito, puesto que la nube implica la custodia de los datos. Aunque compartimos la necesidad de asegurar la facultad de recuperar los datos y la información en un formato exportable a otros proveedores por el cliente, la aplicación analógica del contrato de depósito decae cuando, como se ha ejemplificado anteriormente, los proveedores recogen en los términos del contrato la propiedad de los datos alojados, sobre todo, los que ofrecen el servicio sin remuneración económica. Esta dificultad se vuelve a manifestar en los datos que son generados en el desarrollado del servicio por la interactuación de los clientes, como los metadatos. A falta de un marco

[547] Véase Capítulo III.b.ii: "contrato de alojamiento".

[548] ROSSELLÓ RUBERT, Francisca María: "Modificación, suspensión y extinción del contrato de *Cloud Computing"*, *Cloud computing. Régimen Jurídico para Empresarios,* 2018, Thomson Reuters Aranzadi, p. 371-372.

legal seguro, la regulación contractual deviene imprescindible[549], pudiendo configurarse como un servicio adicional con un coste añadido[550].

Se ha tratado la posibilidad de recuperar los datos de la nube extinta la relación contractual, pero, seguidamente, debe estudiarse qué sucede con los datos que ostenta el proveedor. En el análisis de las cláusulas específicas del contrato de la nube hemos analizado cómo los proveedores pueden no establecer reglas lo suficientemente claras en el borrado de los datos innecesarios, siendo especialmente pernicioso cuando estos tienen diferentes copias de los datos trasladados a la nube (por ejemplo, los conocidos centros de datos imagen). Por lo tanto, habrá que ser especialmente cautelosos en analizar el proceso de borrado y destrucción de los datos.

Se ha defendido que la destrucción del *hardware* es el medio más garantista, si bien, comercialmente es poco viable que un proveedor de servicios acuda a este proceso por los costes asociados. Por lo tanto, deberá atenderse a medidas de sobreescritura de datos, siendo especialmente interesantes y relevantes cuando el cliente obtenga la certeza de la realización del proceso, principalmente a través de certificados. La prueba sobre la realización del proceso de borrado por parte del proveedor del servicio se configura como una medida necesaria y principal finalizada la relación contractual. Independientemente de los datos que el cliente haya trasladado a la nube, más si cabe cuando son de carácter confidencial, son considerados personales o tienen incidencia directa en su modelo de negocio, la búsqueda de algún mecanismo de prueba, como la certificación de alguna

[549] El artículo 13 (39.c) y el artículo 16 (61.b) de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales, COM/2015/0634 final, insta al proveedor a facilitar *"los medios técnicos para recuperar todos los contenidos facilitados por el consumidor, así como cualquier otro dato producido o generado mediante el uso por el consumidor de los contenidos digitales, en la medida en que estos hayan sido retenidos por el proveedor. El consumidor tendrá derecho a recuperar los contenidos sin cargo alguno, sin mayores inconvenientes, en un plazo de tiempo razonable y con un formato de datos utilizado habitualmente"*. Si bien, esta prerrogativa se circunscribe al contratante que tenga la consideración de consumidor. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52015PC0634. Último acceso: 08.08.2018.

[550] Como bien señala ROSELLÓ RUBERT, hay que distinguir entre datos considerados de carácter personal y datos no personales. La recuperación de los primeros, por la aplicabilidad del RGPD y el establecimiento de los derechos de recuperación, portabilidad y supresión que tiene todo interesado, debe considerarse parte de la obligación principal de custodia. ROSSELLÓ RUBERT, Francisca María: "Modificación, suspensión y extinción del contrato de *Cloud Computing"*, *Cloud computing. Régimen Jurídico para Empresarios,* 2018, Thomson Reuters Aranzadi, p. 374.

entidad independiente, garantizará y dará seguridad de que se respeta la confidencialidad e integridad del servicio[551].

Dicho lo anterior, cabría plantearse si el proveedor de los servicios en la nube tiene la obligación de proceder al borrado de los datos finalizada la relación. A falta de una disposición al respecto en el contrato entre las partes, habría que analizar, desde nuestro punto de vista, las obligaciones del proveedor en el contrato de *cloud*. A lo largo del presente trabajo se ha puesto de manifiesto que el prestador de la nube tiene que garantizar la disponibilidad del servicio, la integridad y la confidencialidad de los datos y el desarrollo de políticas de seguridad que custodien los datos que el cliente le confía. Por otra parte, en materia de protección de datos, la normativa conforma al cliente como responsable del tratamiento, al dictaminar la finalidad del tratamiento. Por consiguiente, sobre la base de la buena fe contractual y la naturaleza del contrato conforme al uso, artículos 50 del CCo y 1.258 del CC, el proveedor debe actuar garantizando que los datos trasladados a la nube, al menos, no pueden ser utilizados conforme a su interés, es decir, sin permiso, extinta la relación contractual. Esta exigencia se refrenda en la capacidad técnica del proveedor de la nube de emplear los instrumentos y herramientas necesarias para garantizar la inaccesibilidad de los datos[552]. Por lo tanto, el borrado, según lo expuesto, se considera una medida garantista para preservar el deber de custodia, integridad y confidencialidad extinta la relación contractual, si bien, no como una obligación principal. Un supuesto de hecho completamente distinto se produce en el ejercicio, por el interesado, de los derechos que le confiere el RGPD, principalmente el

[551] En materia de protección de datos personales ya se ha indicado que el RGPD promueve los mecanismos de certificación, como instrumento para garantizar la adecuación del responsable y encargado del tratamiento a la normativa.

[552] ROSELLÓ RUBERT vuelva a aplicar, analógicamente, las disposiciones sobre la figura del depósito. Es decir, el depositario no puede servirse de la cosa depositada sin permiso expreso (artículo 1.767 del CC) y la cosa será devuelta con todos sus productos y accesiones (artículo 1.770 del CC). ROSSELLÓ RUBERT, Francisca María: "Modificación, suspensión y extinción del contrato de *Cloud Computing"*, *Cloud computing. Régimen Jurídico para Empresarios,* 2018, Thomson Reuters Aranzadi, p. 398-399. Aunque posteriormente argumenta que el borrado de datos no entraría a formar parte de las obligaciones principales de la naturaleza jurídica del contrato de la nube por considerar que solo reside el deber de custodia. A nuestro parecer, la aplicación análoga del artículo 1.770 del CC implica, cuanto menos, la posibilidad de facilitar la exportación completa, lo que implicaría, al menos de forma parcial, la limpieza de datos en los sistemas del proveedor.

derecho de supresión o cancelación. En estos supuestos, responsable y encargado se ven compelidos a la supresión de los datos personales[553].

b. La protección del consumidor en el contrato de *cloud computing*

La trascendencia del consumidor en la contratación de los servicios del *cloud* tiene su proyección en el régimen jurídico aplicable. Por una parte, por la particularidad de quién requiere los servicios de computación en la nube y la especial protección que la normativa europea y nacional proyecta y, por otra, por el canal habitual donde se desarrolla la contratación de los servicios. En consecuencia, debe compatibilizarse el régimen jurídico establecido para el comercio electrónico y la protección jurídica a los consumidores y usuarios.

La contratación del *cloud computing* por parte del cliente[554] supera el ámbito jurídico nacional en la mayoría de los supuestos, la oferta se distribuye en grandes cuotas de mercado que copan grandes proveedores internacionales. En este marco, la autonomía de la voluntad, como fuente primordial del Derecho de obligaciones, juega un papel fundamental para el entendimiento entre las partes[555]. Sin embargo, la eficacia y validez de las cláusulas estarán condicionadas al cumplimiento de la normativa aplicable. VEGA VEGA[556] argumenta que las redes telemáticas y las nuevas tecnologías han permitido establecer relaciones descontextualizadas o sin presencia física jurídicamente relevante. En este contexto, las cláusulas no negociadas individualmente o predispuestas por los operadores económicos se incorporan a contratos tipos o de adhesión a celebrar con los consumidores y usuarios, práctica habitual en la contratación electrónica. El poder de

---

[553] Artículo 28.3.g del RGPD: *"a elección del responsable, suprimirá o devolverá* (encargado) *todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros"*.

[554] En este apartado trataremos indistintamente el concepto de cliente, consumidor y usuario, salvo que se indique lo contrario.

[555] ÁLVAREZ DE SOTOMAYOR, Silvia Feliu: "Nulidad de las cláusulas de jurisdicción y ley aplicable a la luz de la Ley 3/2014 por la que se modifica el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios", *Revista electrónica de estudios internacionales (REEI)*, 2015, nº 29, p. 2. Accesible en: http://www.reei.org/index.php/revista/num29/archivos/Estudio_FELIU_Silvia.pdf. Último acceso: 08.08.2018.

[556] VEGA VEGA, José Antonio: "Las condiciones generales en la contratación electrónica", *Revista de Contratación Electrónica*, 2009, nº 101, p. 16.

imposición, en la contratación de los servicios, de los proveedores de *cloud* se ve reforzado, debiendo el ordenamiento jurídico velar por la parte más débil de la relación contractual y así reestablecer el desequilibrio producido. Este es el hándicap del consumidor que quiere utilizar el servicio, ya sea a través de una contraprestación económica o sin cargo[557]. Se encuentra con unas condiciones impuestas por el proveedor del servicio, sin posibilidad de negociación, con conocimientos técnicos y jurídicos insuficientes para valorar de forma holística el servicio ofrecido y las condiciones que le serán aplicables. En palabras de ROYO MARTÍNEZ[558], que a pesar del lapso temporal siguen estando plenamente vigentes, *"... con su ficción del hombre que siempre sabe muy bien lo que quiere y siempre puede escoger a su arbitrio entre contratar o buscar a través de la competencia mejores condiciones"* los legisladores no tuvieron la perspicacia *"de prever los resultados de las grandes concentraciones de capital ni las consecuencias de valor ingente, cuya magnitud, cuando no una previa concesión administrativa, les proporcionaba un monopolio, al menos de hecho..."*.

Los potenciales problemas a los que se enfrenta el consumidor en el uso de la nube no disienten, en gran medida, a los que afrontan las empresas que deciden contratar el servicio. De forma generalizada, la naturaleza jurídica del servicio utilizado, la transparencia de los términos en la contratación, la fiabilidad y seguridad del servicio, la correcta protección de los datos personales aportados por el cliente, los supuestos de subcontratación del servicio, los diferentes usos y accesos a los datos cargados en la nube y los derechos y obligaciones que asisten al cliente y al proveedor del servicio son las cláusulas comunes a analizar, coincidiendo, en gran medida, con la regulación impuesta para el B2B.

A las consideraciones expuestas, se ha de añadir, que en numerosas ocasiones resulta difícil distinguir cuando se utiliza la nube para un uso comercial o privado. El cliente puede empezar probando un servicio para fines personales y, una vez adquirida la destreza suficiente, combinar la herramienta informática para usos empresariales. Este puede ser el caso de un pequeño empresario que se inicia en el servicio, a través de proveedores que

[557] Ya hemos indicado que, aunque el servicio se autodefina como "gratuito", tiene costes asociados: publicidad, utilización de datos del usuario, acopio de las experiencias del cliente…

[558] ROYO MARTÍNEZ, Miguel: "Contratos de Adhesión", *Anuario de Derecho Civil,* 1949, p. 54. Accesible en: https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-C-1949-10005400070_ANUARIO_DE_DERECHO_CIVIL_Contratos_de_adhesi%F3n. Último acceso: 08.08.2018.

ofrecen la nube sin coste o por una pequeña cantidad económica, y una vez adaptado incorpora datos relacionados con el desarrollo de su actividad empresarial. También puede suceder que se revierta el condicionante que inicia el uso del *cloud*, es decir, usuarios que acostumbrados a la nube en su quehacer diario de su prestación laboral o empresarial empiezan a utilizar la herramienta para usos privados. Ese uso mixto de la aplicación dificulta la aplicabilidad de la normativa tuitiva al consumidor y usuario, lo que obliga a delimitar el ámbito de aplicación.

La Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo[559], con vocación a proteger al consumidor antes de la efectiva contratación con el proveedor de servicios (imponiendo obligaciones al prestador para que el cliente pueda conocer de forma clara, comprensible y de fácil acceso la información relativa a los términos y condiciones del servicio y contrato); la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)[560], que impone la transparencia en el comercio electrónico; así como la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores[561], buscando una relación equitativa entre consumidor y proveedor celebrado el contrato, son ejemplos de la preocupación del legislador en proporcionar a los consumidores un régimen jurídico garantista, siendo aplicable a estos servicios informáticos. Es necesario generar confianza al consumidor para que pueda emplear el medio electrónico en la contratación, y en segundo lugar, apostar por el servicio de la nube. Una protección similar a las transacciones tradicionales, con unos estándares

[559] Accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2011-82312. Último acceso: 08.08.2018.

[560] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32000L0031 y https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295. Últimos acceso: 08.08.2018.

[561] Accesible en:http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31993L0013&from=ES Último acceso: 08.08.2018.

mínimos de protección, basados en la buena fe y la confianza, impulsará la adopción del *cloud computing*.

Sirva para atestiguar la relevancia del comercio electrónico y la necesaria protección de los consumidores en la contratación de los servicios de *cloud* por este medio, lo dispuesto en el Considerando 7 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, sobre el comercio electrónico: "*es fundamental para garantizar la seguridad jurídica y la confianza de los consumidores que la presente Directiva establezca un marco claro y de carácter general para determinados aspectos jurídicos del comercio electrónico en el mercado interior*".

a. Definición de consumidor a la luz de la normativa aplicable.

Para delimitar el ámbito de aplicación de las normas protectoras de los consumidores de la nube, debemos determinar, en primer lugar, qué debe considerarse "consumidor".

En una primera aproximación, concepto generalizado que puede tener la sociedad, podemos considerar consumidor a toda persona física o jurídica que actúa en el mercado fuera de su capacidad profesional o de los negocios relacionados con el mismo. A pesar de esta idea general, no es un término unívoco, dependiendo del marco jurídico en el que se emplee.

El Reglamento (UE) nº 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[562], Bruselas I bis, determina en su artículo 17 que el consumidor es aquella persona que celebra contratos *"para un uso que pueda considerarse ajeno a su actividad profesional"*. Definición que coincide, por razón de la materia, con lo establecido en el artículo 13[563] del Convenio de Bruselas de 1968, relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia

[562] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32012R1215 y https://www.boe.es/doue/2012/351/L00001-00032.pdf. Últimos accesos: 08.08.2018.

[563] *"En materia de contrato concluido por una persona para un uso que pudiera considerarse como ajeno a su actividad profesional, a partir de ahora denominada " el consumidor "..."*.

civil y mercantil[564]. El Convenio de Roma de 1980 sobre la ley aplicable a las obligaciones contractuales[565] comparte acepción[566]. Sin embargo, la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores[567] define a los consumidores como *"personas físicas que actúan fuera de su actividad comercial, empresa, oficio o profesión"*. Definición que recogía la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, sobre comercio electrónico[568] y que parte del artículo 1.2.a) de la Directiva 1999/44/CE del Parlamento Europeo y del Consejo, de 25 de mayo de 1999, sobre determinados aspectos de la venta y las garantías de los bienes de consumo[569], al definir al consumidor como "*toda persona física que, en los contratos a que se refiere la presente Directiva, actúa con fines que no entran en el marco de su actividad profesional"*. La precisión de persona física está presente, también, en la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores[570], artículo 2.b)[571], y en la derogada Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a

---

564 Accesible en: https://www.boe.es/boe/dias/1994/10/20/pdfs/A32815-32829.pdf y http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:41968A0927(01)&from=ES. Últimos accesos: 08.08.2018.

565 Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:41980A0934. Último acceso: 08.08.2018.

566 Artículo 5.1: *"El presente artículo se aplicara a los contratos que tengan por objeto el suministro de bienes muebles corporales o de servicios a una persona, el consumidor, para un uso que pueda ser considerado como ajeno a su actividad profesional, así como a los contratos destinados a la financiación de tales suministros"*.

567 La Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo. Enlace de acceso ya referenciado.

568 Artículo 2.e): *"'consumidor': cualquier persona física que actúa con un propósito ajeno a su actividad económica, negocio o profesión"*.

569 Accesibles en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31999L0044 y https://www.boe.es/buscar/doc.php?id=DOUE-L-1999-81346. Últimos accesos: 08.08.2018.

570 Accesibles en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31993L0013 y https://www.boe.es/buscar/doc.php?id=DOUE-L-1993-80526. Últimos accesos: 08.08.2018.

571 *"« consumidor »: toda persona física que, en los contratos regulados por la presente Directiva, actúe con un propósito ajeno a su actividad profesional"*.

distancia[572] (derogada por la Directiva sobre los derechos de los consumidores), artículo 2.2[573]. Coincidiendo con CARBALLO FIDALGO[574], la alusión expresa a "persona física" es deliberada, tanto por su reiteración en los instrumentos normativos expuestos, como por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas[575]. La Corte ha optado por una interpretación estricta del concepto de consumidor, recalcando su carácter excepcional en la aplicación y subrayando la consideración de ser la parte económica y jurídicamente más débil y menos experta. Por lo tanto, restringe la posibilidad a que personas jurídicas ajenas a actividades profesionales (asociaciones o comunidades de bienes, por ejemplo) puedan acogerse a la protección auspiciada para el consumidor, aun cuando su poder de negociación e inferioridad en el mercado, de forma técnica y económica, sea similar. Esta limitación, como posteriormente veremos, no se recoge en la normativa española.

El Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLCU)[576], tras la reforma introducida por la Ley 3/2014[577], de 27 de marzo, define al consumidor y usuario, artículo 3, como *"…las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. Son también consumidores a efectos de esta norma las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial"*. El legislador español ha disipado dudas y reconoce

[572] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31997L0007. Último acceso: 08.08.2018.

[573] *"«consumidor»: toda persona física que, en los contratos contemplados en la presente Directiva, actúe con un propósito ajeno a su actividad profesional"*.

[574] CARBALLO FIDALGO, Marta: "Marco normativo. Derecho comunitario e interno", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch, p. 23-24.

[575] Entre otras, la Sentencia del Tribunal de Justicia de las Comunidades Europeas (Sala Tercera), del 22 de noviembre de 2001, en los asuntos acumulados C-541/99 y C-542-99. Accesible en: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=46869&pageIndex=0&doclang=ES&mode=lst. Último acceso: 08.08.2018.

[576] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555. Último acceso: 08.08.2018.

[577] En la redacción originaria ya se recogía la posibilidad de considerar a las personas jurídicas como consumidores, si bien de una forma parca: *"son consumidores o usuarios las personas físicas o jurídicas que actúan en un ámbito ajeno a una actividad empresarial o profesional"*.

expresamente dentro del concepto de consumidor a las personas jurídicas que actúan ajenas a una actividad empresarial o profesional, siempre sin ánimo de lucro[578]. De esta forma, se positiviza la consideración establecida por nuestros juzgados y tribunales[579]. Asociaciones, cooperativas, fundaciones e incluso entes sin personalidad jurídica que contraten sin ánimo de lucro y al margen de la actividad comercial o empresarial deberán ser consideradas consumidores, al presentar frente al empresario inferioridad en términos jurídicos, económicos y técnicos. La posibilidad de que las personas jurídicas actúen como consumidores la plantean, en el marco comunitario, CUNNINGHAM y REED[580]. Relacionan el grado profesional o comercial implicado en la prestación de un servicio o un bien para determinar si la actuación de la persona jurídica en la contratación de la nube puede enmarcarse en las normas de defensa del consumidor. Concluyen que, cuando se contrate un servicio de *cloud* que no afecte al negocio, se considerará, a efectos jurídicos, como consumidor. Como posteriormente veremos, por el desarrollo de la nube, esta

[578] BERCOVITZ RODRIGUEZ-CANO señala, no obstante, que la propia Ley a la hora de determinar los puntos de conexión para la aplicación de las normas de protección en materias de garantía (artículo 67.3.2º parraf.) vincula el consumidor con un ciudadano, por lo tanto, a una persona física. BERCOVITZ RODRIGUEZ-CANO, Rodrigo: "Comentario al art. 3 de la TRLGDCU", *Comentario del Texto Refundido de la Ley General para la defensa de los consumidores y usuarios y otras leyes complementarias*, 2015, Aranzadi. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

[579] La Sentencia de la Audiencia Provincial de Huelva (Sección 3ª), del 21 de marzo de 2014, número de recurso 151/2013, indica *"la inclusión y protección a las personas jurídicas, no debe resultarnos extraña, ya que la finalidad de la normativa de protección del consumidor no es proteger a una determinada categoría de sujetos, sino garantizar el equilibrio contractual cuando las condiciones de mercado no bastan para ello, y ese desequilibrio debe evaluarse en el momento en que se formaliza un contrato específico"* (Fundamentos de Derecho – Previo). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7039133&links=Huelva&optimize=20140508&publicinterface=true. Último acceso: 08.08.2018. La Sentencia de la Audiencia Provincial de Guipúzcoa (Sección 3ª), del 12 de junio 2000, número de recurso 3306/1999, explicita que *"dado que para que una persona jurídica pueda ser conceptuada como consumidora debe recurrir los mismos requisitos que el consumidor persona física y por ello, será necesario que se trate de una persona jurídica que no tenga por objeto o que no realice de hecho una actividad de producción o de comercialización de bienes o servicios para el mercado, deberá ser, por tanto, como en el supuesto que nos ocupa, una persona jurídica sin finalidad de lucro y que en su caso, transmita a título gratuito los bienes o servicios adquiridos"*. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=2349943&links=Guipuzcoa&optimize=20040524&publicinterface=true. Último acceso: 08.08.2018. La Sentencia del Tribunal Supremo, del 30 de noviembre de 1996, número de recurso 319/1996, considera consumidor a un ente sin personalidad jurídica. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2942125&links=&optimize=20031203&publicinterface=true. Último acceso: 08.08.2018.

[580] CUNNINGHAM, Alan; y REED, Chris: "Caveat Consumer? – Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud", *Queen Mary University of London - Legal Studies Research Paper*, 2013, nº 130, p. 18-19. Accesible en: https://ssrn.com/abstract=2202758. Último acceso: 08.08.2018.

argumentación está relacionada con el uso mixto del servicio (ejecución de una actividad comercial y uso privado del *cloud*), aunque no es estrictamente necesario un uso mixto de la nube para cumplir las condiciones establecidas en el ámbito de aplicación subjetivo.

En este epítome estamos tratando el concepto de consumidor en sentido técnico jurídico, es decir, consumidor contratante. La redacción de 1984 de la Ley de defensa de los consumidores y usuarios[581], no distinguía entre el consumidor jurídico y el material (artículo 1.2: *"...utilizan o disfrutan como destinatarios finales, bienes muebles o inmuebles, productos, servicios, actividades o funciones..."*), desechándose tal concepción de consumidor en las futuras reformas, posibilitando considerar consumidor a quien, como indica ÁLVAREZ MORENO[582], introduce o reintroduce bienes o servicios en el mercado, siempre que sea ajeno a una actividad profesional[583]. Aunque de difícil aplicación en el comercio de la nube, siempre se ha de tener presente.

Teniendo presente, como se ha expuesto, que no existe una noción unitaria de consumidor, por lo que se deberá analizar el ámbito subjetivo de aplicación de la normativa de estudio, de forma genérica adoptaremos el concepto establecido en el TRLCU. Conceptos especiales, como consumidor vulnerable, expuesto por la Directiva 2011/83/UE de derechos de los consumidores, y 2005/29/UE sobre prácticas desleales, exigen un deber especial de información por parte del proveedor de servicio.

i. Consumo mixto

El *cloud computing* posibilita a los ciudadanos acceder a información, documentos, archivos, programas…, desde cualquier dispositivo, mediante una simple conexión a Internet. La evolución de la nube ha introducido en el mercado servicios con un bajo coste económico o incluso gratuitos. Estos condicionantes han propiciado que los ciudadanos

---

[581] Ley 26/1984, de 19 de julio, Ley General para la Defensa de los Consumidores y Usuarios. Accesible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1984-16737. Último acceso: 08.08.2018.

[582] ÁLVAREZ MORENO, María Teresa: "Ámbito de aplicación subjetivo", *Protección jurídica del consumidor en la contratación en general: normas imperativas y pactos al respecto*, 2015, Reus, p. 24.

[583] Postura criticada por parte de la doctrina, que sigue exigiendo el criterio positivo y negativo en la caracterización del consumidor (destinatario final, sin incorporarlos al mercado y ajeno a la actividad profesional). Entre otros, CARBALLO FIDALGO, Marta: "Ámbito de aplicación del régimen legal sobre cláusulas abusivas", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch, p. 64; y CÁMARA LAPUENTE, Sergio: "Artículos 1 a 7", *Comentarios a las normas de protección de los consumidores. Texto refundido (RDL 1/2007) y otras leyes y reglamentos vigentes en España y en la Unión Europea*, 2011, Colex, p. 116-120.

utilicen la mejora tecnológica combinando un uso profesional y privado de la herramienta. Sirva de ejemplo, el pequeño comerciante que empieza utilizando un servicio en nube, que incluye correo electrónico, para uso privado. Habituado a las facilidades que ofrece, realiza comunicaciones comerciales o envía publicidad a su red de clientes. *Mutatis mutandis*, igual sucede con esos profesionales que posteriormente utilizan la nube para un uso privado. Debe añadirse que, además de lo citado, el uso mixto de la nube no suele conocerse *ex ante*, es decir, en el momento de la celebración del contrato.

El Tribunal de Justicia de las Comunidades Europeas en la sentencia de 3 de julio de 1997, caso Francesco Benincasa contra Dentalkit Srl[584], y en la sentencia de 20 de enero de 2005, caso Johann Gruber contra Bay Wa AG[585], trataba el uso mixto, como operador económico/consumidor. De una lectura conjunta, puede destacarse como el Tribunal de Justicia reitera que las reglas especiales que garantizan la protección del consumidor deben interpretarse de manera restrictiva, en un contrato determinado, en función de la naturaleza y la finalidad del contrato, y no respecto a la situación subjetiva de la persona en concreto. La búsqueda de una protección adecuada para la parte del contrato considerada económicamente más débil, con menor experiencia y conocimiento jurídico, dota al consumidor de las herramientas adecuadas para el equilibrio entre partes. Por lo tanto, en los supuestos de un uso mixto, el sujeto deberá ser considerado consumidor cuando el objetivo profesional o comercial sea limitado, pueda considerarse insignificante, siendo el uso privado predominante en el desarrollo de la prestación. En palabras de BERCOVITZ RODRIGUEZ-CANO[586], *"en tales actuaciones mixtas el adquirente solo merece la protección propia de los consumidores cuando el destino manifiestamente predominante del bien o servicio adquirido sea para un uso o disfrute*

[584] Sentencia del Tribunal de Justicia de las Comunidades Europeas (Sala Sexta), del 03 de julio de 1997, en el asunto C-269/95, Francesco Benincasa contra Dentalkit Srl. Accesible en: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=43682&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=550885. Último acceso: 08.08.2018.

[585] Sentencia del Tribunal de Justicia de las Comunidades Europeas (Sala Segunda), del 20 de enero de 2005, en el asunto C-464/01, Johann Gruber contra Bay Wa AG. Accesible en: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=49857&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=550885. Último acceso: 08.08.2018.

[586] BERCOVITZ RODRIGUEZ-CANO, Rodrigo: "Comentario al art. 3 de la TRLGDCU", *Comentario del Texto Refundido de la Ley General para la defensa de los consumidores y usuarios y otras leyes complementarias*, 2015, Aranzadi. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

particular, mientras que el destino profesional o empresarial sea manifiestamente menor, esto es, residual".

Esta solución aparece actualmente en la Directiva 2011/83/UE sobre derecho de los consumidores, en la Exposición de Motivos. Así, *"en el caso de los contratos con doble finalidad, si el contrato se celebra con un objeto en parte relacionado y en parte no relacionado con la actividad comercial de la persona y el objeto comercial es tan limitado que no predomina en el contexto general del contrato, dicha persona deberá ser considerada como consumidor"*.

El Tribunal Supremo se ha pronunciado sobre el uso mixto en la Sentencia de 5 de abril de 2017[587], tomando en consideración el criterio interpretativo de la Directiva desarrollado por la doctrina comunitaria.

El marco normativo expuesto configura una protección al consumidor basada en una defensa *ex ante* del contrato. Sin embargo, el carácter restrictivo de la aplicación limita, ante un uso mixto de la nube, basarse en las intenciones o propósitos del cliente para considerar al demandante consumidor. Se agrava, además, con el carácter de contratación masiva y el uso de cláusulas de adhesión empleadas en el sector. CUNNINGHAM y REED[588] señalan dos posibilidades para dictaminar si nos encontramos en un contrato de la nube con consumidores: delimitar por la naturaleza del servicio su finalidad o no de consumo, por ejemplo, por la potencia requerida y/o por las prestaciones de servicio solicitadas; o, ante servicios que pueden ser usados indistintamente para consumo privado como profesional o comercial, ser el proveedor quien solicite la finalidad del servicio al cliente, con el riesgo de asumir una actuación fraudulenta por parte del contratante. Se ha de añadir que, en esta labor de fiscalización, que recae en el proveedor, deben tenerse presente algunos indicios que facilitan la determinación de un uso propio o empresarial: razón social con la que se contrata, redireccionamientos electrónicos a dominios de titularidad empresarial, y usuarios que tienen acceso o direcciones, físicas y electrónicas, con las que se identifica el cliente.

---

[587] Sentencia del Tribunal Supremo, del 05 de abril de 2017, número de resolución 224/2017. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7992000&links=uso%20mixto&optimize=20170419&publicinterface=true. Último acceso: 08.08.2018.

[588] CUNNINGHAM, Alan; y REED, Chris: "Caveat Consumer? – Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud", *Queen Mary University of London - Legal Studies Research Paper*, 2013, nº 130, p. 18. Accesible en: https://ssrn.com/abstract=2202758. Último acceso: 08.08.2018.

b. Cláusulas generales de contratación, cláusulas no negociadas individualmente y cláusulas de protección al consumidor.

En la contratación del *cloud computing*, y en general en todos los contratos informáticos, en el cual los consumidores son parte contratante, se mezclan conceptos no coincidentes que suelen ser utilizados como sinónimos.

Las cláusulas generales de contratación son condiciones que se incorporan al contrato, entre empresarios o con consumidores y usuarios, predispuestas, con la finalidad de ser incorporadas a una pluralidad de contratos, sin importar la apariencia externa, siendo consideradas aisladamente, es decir, sin importar que otras cláusulas se negocien de manera individual[589]. Como señala PÉREZ ESCOLAR[590], el objetivo que persigue la regulación de las condiciones generales de contratación es la protección de cualquier adherente, sea empresario o consumidor, frente a un empresario o profesional predisponente. Las características señaladas aparecen en el ámbito objetivo, artículo 1, de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación[591] (LCGC). Estas son predisposición, incorporación unilateral, pluralidad e incorporación al contrato. El concepto de condiciones generales de contratación es extensible a todo el ordenamiento jurídico español, no solo a los efectos de la LCGC, relevante por la prolija regulación autonómica al respecto[592]. Por consiguiente, las consecuencias de contradecir cualquier norma imperativa o prohibitiva será la nulidad de pleno derecho de las condiciones generales, salvo que establezca un efecto distinto. La buena fe contractual establecida en el artículo 1.258 del CC se manifiesta como norma de validez cuando el adherente sea un consumidor, artículo 82.1 del TRLCU, sin embargo, no es extensible cuando sea un empresario o profesional el contratante del servicio, al tratarse de normas

[589] CARRASCO PERERA, Ángel: "Control de validez de condiciones generales y cláusulas abusivas", *Derechos de contratos,* 2017, Aranzadi. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

[590] PÉREZ ESCOLAR, Marta: "Incorporación al contrato de cláusulas no negociadas: perspectivas de reforma a la luz del panorama europeo, la Propuesta de Modernización del Código civil y el Anteproyecto de Ley de Código mercantil", *Anuario de Derecho Civil*, 2015, Vol. 68, nº 2, p. 419.

[591] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-1998-8789. Último acceso: 08.08.2018.

[592] MARÍN LÓPEZ, Juan José: "El ámbito de aplicación de la Ley sobre condiciones generales de la contratación", *Condiciones Generales de la Contratación y Cláusulas Abusivas*, 2000, Lex Nova, p. 126; y PARDO GATO, José Ricardo: "Las condiciones generales de la contratación y el listado de cláusulas abusivas", *Las cláusulas abusivas en los contratos de adhesión*, 2004, Dijusa, p. 106.

de derecho contractual dispositivo[593]. Es decir, la buena fe contractual establecida de modo genérico en el artículo 1.258 del CC, y para los contratos mercantiles en el artículo 57 del CCo, es aplicable, incluso, cuando la contratación es entre empresarios o profesionales, si bien a efectos de su consideración para determinar si una cláusula es abusiva, artículo 82.1 del TRLCU, solo es aplicable cuando el contratante es un consumidor o usuario. No es óbice para que la transgresión de la buena fe puede dar fundamento jurídico a la contraparte para actuar contra el transgresor. Siguiendo a PERTÍÑEZ VILCHEZ[594], en el estudio de la buena fe contractual entre empresarios, *"el art. 1.258 CC es una norma de integración del contenido del contrato con obligaciones no pactadas que derivan de la buena fe, pero no una norma que establezca criterios para enjuiciar la validez de contenidos contractuales"*[595].

Cuando una persona intenta contratar un servicio de la nube, como en reiteradas ocasiones se ha puesto de manifiesto, raramente puede negociar individualmente alguna de las cláusulas del contrato. Incluso en el supuesto de incorporar alguna cláusula negociada individualmente, como se ha señalado, deberá tenerse por cláusulas generales de contratación las restantes disposiciones, siendo de aplicación, por tanto, LCGC al resto del contrato. La problemática reside en que, si la parte contratante es un consumidor, el control de las cláusulas no se basa solo en la LCGC, sino que hay que acudir a los dictados del TRLCU, al tratarse de cláusulas que no han sido individualmente negociadas[596]. El

[593] Sin embargo, la consecuencia jurídica puede ser extensibles a la contratación entre empresarios cuando haya cláusulas que condicionen el contrato a la potestad de una sola parte, se condicione el cumplimiento al arbitrio del obligado o el objeto del contrato se remita al arbitrio de una parte posterior a la formación, conforme al artículo 1.115, 1.256 y 1.447 del Código civil. El TRLCU concreta, para los consumidores, las anteriores disposiciones en parte de su clausulado, como, por ejemplo, en el artículo 85.5, 86.8 o 87.3.

[594] PERTÍÑEZ VÍLCHEZ, Francisco: "Buena fe ex art. 1.258 cc y nulidad de las cláusulas suelo sorpresivas en contratos de préstamo con adherentes empresarios", *Indret: Revista para el Análisis del Derecho,* 2016, número 4, p. 12. Accesible en: http://www.indret.com/pdf/1266_es.pdf. Último acceso: 08.08.2018.

[595] Así lo ha declarado, entre otras, la Sentencia del Tribunal Supremo, del 30 de abril de 2015, número de recurso 929/2013, FD Quinto: *"el art. 1258 del Código Civil que se invoca por el recurrente contiene reglas de integración del contrato, en concreto la relativa a la buena fe, de modo que en el cumplimiento y ejecución del contrato pueda determinarse lo que se ha denominado el "contenido natural del contrato". Pero con base en este precepto no puede pretenderse que se declare la nulidad de determinadas condiciones generales que deban ser expulsadas de la reglamentación contractual y tenidas por no puestas, y que, en su caso, puedan determinar la nulidad total del contrato"*. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7385947&links=1258&optimize=20150521&publicinterface=true. Último acceso: 08.08.2018.

[596] Los artículos 80 y ss. del TRLCU regulan los requisitos de incorporación de las cláusulas no negociadas individualmente.

concepto que emplea el TRLCU no coincide con el definido por la LCGC. Para determinar qué debe entenderse como "cláusulas no negociadas individualmente" debemos acudir a la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores[597]. El artículo 3.2 de la citada Directiva establece que *"se considerará que una cláusula no se ha negociado individualmente cuando haya sido redactada previamente y el consumidor no haya podido influir sobre su contenido, en particular en el caso de los contratos de adhesión"*. La definición solo exige que el consumidor firme el contrato con las cláusulas, o la cláusula, predispuestas, independiente a cualquier negociación posible por el profesional o empresario. Es decir, que firme un contrato de adhesión. Podemos traducirlo en que habrá cláusulas que estén protegidas por las normas establecidas por el TRLCU pero no por la LCGC, al tratarse un contrato de adhesión particular[598].

En la práctica de la contratación de la nube, los consumidores usualmente utilizarán los medios electrónicos para adquirir el servicio. Los proveedores establecerán las condiciones generales de contratación, y las cláusulas predispuestas, como instrumento para ofertar sus servicios. Antes de entrar en los requisitos de incorporación de las citadas condiciones y cláusulas por la normativa, el artículo 80 del TRLCU establece como requisitos para la correcta incorporación de las cláusulas no negociadas individualmente con los consumidores, basados en la buena fe y el equilibrio entre los derechos y

---

[597] Accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1993-80526. Último acceso: 08.08.2018.

[598] Así lo establece la propia LCGC:

E.M. Preámbulo, párrafo 5º de la LCGC: *"Una cláusula es condición general cuando está predispuesta e incorporada a una pluralidad de contratos exclusivamente por una de las partes, y no tiene por qué ser abusiva. Cláusula abusiva es la que en contra de las exigencias de la buena fe causa en detrimento del consumidor un desequilibrio importante e injustificado de las obligaciones contractuales y puede tener o no el carácter de condición general, ya que también puede darse en contratos particulares cuando no existe negociación individual de sus cláusulas, esto es, en contratos de adhesión particulares"*.

E.M. VIII, párrafo 6º: *"La regulación específica de las cláusulas contractuales en el ámbito de los consumidores, cuando no se han negociado individualmente (por tanto también los contratos de adhesión particulares), no impide que cuando tengan el carácter de condiciones generales se rijan también por los preceptos de la Ley de Condiciones Generales de la Contratación"*.

Para ahondar más en la distinción entre cláusulas generales de contratación y cláusulas de adhesión particulares se recomienda: ROMAN LLAMOSI, Sofía: "Los contratos bancarios – Aumento litigiosidad y respuesta de los tribunales", *Revista de Derecho vLex,* 2015, núm. 131. Acceso a través de vLex digital (requiere suscripción)

obligaciones entre las partes, que como veremos determinará el carácter abusivo de las cláusulas, los siguientes:

- Una redacción concisa de las cláusulas, con una redacción que posibilite su comprensión, siendo necesario un lenguaje claro y sencillo. Añade, la normativa, que no debe procederse a *"reenvíos a textos o documentos que no se faciliten previa o simultáneamente a la conclusión del contrato, y a los que, en todo caso, deberá hacerse referencia expresa en el documento contractual"*.
- Accesibilidad. El consumidor, antes de la celebración del contrato, debe tener la posibilidad de conocer la existencia y contenido de las condiciones por las que se regirá.
- Deben ser legibles, exigiéndose un tamaño de letra adecuado, nunca inferior al milímetro y medio, y un contraste de fondo que no dificulte la lectura.

En este contexto, el propio TRLCU en el artículo 82 y siguientes regula algunas cláusulas abusivas para el consumidor. Sin perjuicio de un estudio pormenorizado de las cláusulas habituales en los contratos de computación en la nube que pueden estar afectadas por la regulación, que procederemos en el siguiente subapartado, se definen como cláusulas abusivas aquellas que no negociadas previamente por las partes, en contra de la buena fe contractual, causen un perjuicio al consumidor y usuario por un desequilibrio importante entre sus derechos y obligaciones[599].

Enmarcadas las posibles cláusulas que pueden estar presentes en los contratos de computación en la nube, delimitados los conceptos de condiciones generales de contratación, de cláusulas no negociadas individualmente y de adhesión, puede evaluarse la incorporación y legalidad de las estipulaciones.

Iniciando el control de validez de las condiciones generales de contratación, los requisitos fundamentales aparecen establecidos en el artículo 5.1 de la LCGC. Se concretan en:

[599] En cláusulas o condiciones particulares también es posible considerar el carácter de abusiva. Véase la Sentencia del Juzgado de lo Mercantil nº 1 de A Coruña, número 256/2016, de 22 de noviembre de 2016. En concreto, el Fundamento de Derecho III. Accesible en: http://www.poderjudicial.es/stfls/TRIBUNALES%20SUPERIORES%20DE%20JUSTICIA/TSJ%20Galicia/DOCUMENTOS%20DE%20INTERES/Jdo%20Mercantil%201%20A%20Coru%C3%B1a%2022%20nov%202016.pdf. Último acceso: 08.08.2018.

- El empresario o profesional que la incorpora debe informar al consumidor, en nuestro caso, de la existencia.
- Se debe hacer referencia en el contrato a las condiciones generales incorporadas.
- Debe facilitarse un ejemplar al adherente.
- El adherente debe aceptar su incorporación y debe ser firmado por todos los contratantes[600].

Debemos traer a colación la obligación previa al proceso de contratación electrónica que impone la LSSICE en el artículo 27.4, *"el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que estas puedan ser almacenadas y reproducidas por el destinatario"*.

Dos requisitos son, por tanto, esenciales para la licitud de las condiciones generales de contratación: la cognoscibilidad y la compresibilidad de las cláusulas.

Los principios rectores en los requisitos de incorporación de las condiciones generales de contratación se encuentran en el artículo 5.4 de la LCGC. Las condiciones generales de contratación se ajustarán a *"los criterios de transparencia, claridad, concreción y sencillez"*. Por lo tanto, las cláusulas que sean *"ilegibles, ambiguas, oscuras e incomprensibles"* se considerarán no incorporadas, a tenor del artículo 7.b), salvo en la excepción que recoge el precepto. Los criterios citados configuran el requisito de compresibilidad y perceptibilidad, aunque expresamente no lo recoja el cuerpo legal indicado. Estos criterios, ante cláusulas no negociadas con los consumidores, se reproducen en el artículo 80.1.a) del TRLCU (*"concreción, claridad y sencillez en la redacción"*).

La legibilidad o comprensibilidad de las condiciones generales de contratación se relacionan directamente con la tipografía, la configuración o la calidad en la visualización

[600] En la práctica contractual del *cloud* podemos encontrarnos con proveedores que las condiciones generales de contratación las fijan en su página web o remiten a un enlace web donde se encuentran recogidas. Siempre que sea necesario que el cliente adopte una postura activa, por ejemplo, marcar una casilla de aceptación o sea obligatorio abrir el *link* antes de finalizar la contratación, deben entenderse cumplidas las premisas legales. En este sentido falla la Audiencia Provincial de Barcelona, sección 15, en la Sentencia núm. 185/2015 de 14 de julio de 2015. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7499474&links=&optimize=20151022&publicinterface=true. Último acceso: 08.08.2018.

o, en menor medida en los contratos electrónicos, con la calidad de la impresión[601]. Como señala PÉREZ ESCOLAR[602], la normativa establece un criterio objetivo para validar la incorporación de una cláusula predispuesta cuando contrata un consumidor. El tamaño de la letra de la cláusula en relación con las restantes cláusulas del contrato (sin resalto, inferior tamaño o negritas, por ejemplo)[603] o su ubicación en lugares secundarios u ocultos invalidan la incorporación de la cláusula[604].

Para los consumidores, el requisito de la compresibilidad aparece como exigencia de información previa al contrato, artículo 60.1 del TRLCU (*"…deberá facilitarle de forma clara y comprensible, salvo que resulte manifiesta por el contexto, la información relevante, veraz y suficiente sobre las características principales del contrato…"*), exigencia que se reproduce para los contratos celebrados a distancia de forma genérica, artículo 98.1 del TRLCU, y en particular para los contratos celebrados por medios electrónicos, artículo 98.2 del TRLCU[605]. Mas en el contrato del *cloud*, debemos tener presente que los sitios web que permitan la contratación del servicio *"deberán indicar de modo claro y legible, a más tardar al inicio del procedimiento de compra, si se aplica alguna restricción de entrega y cuáles son las modalidades de pago aceptadas"*, artículo 98.3.

---

[601] El artículo 80.1.b) del TRLCU establece, como requisito de las cláusulas no negociadas: *"Accesibilidad y legibilidad, de forma que permita al consumidor y usuario el conocimiento previo a la celebración del contrato sobre su existencia y contenido. En ningún caso se entenderá cumplido este requisito si el tamaño de la letra del contrato fuese inferior al milímetro y medio o el insuficiente contraste con el fondo hiciese dificultosa la lectura"*.

[602] PÉREZ ESCOLAR, Marta: "Incorporación al contrato de cláusulas no negociadas: perspectivas de reforma a la luz del panorama europeo, la Propuesta de Modernización del Código civil y el Anteproyecto de Ley de Código mercantil", *Anuario de Derecho Civil*, 2015, Vol. 68, nº 2, p. 429.

[603] Sentencia del Tribunal Supremo de 5 de julio de 1997, núm. 664/1997, FD I (accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=3238960&links=&optimize=20030704&publicinterface=true. Último acceso: 08.08.2018) o Sentencia de la Audiencia Provincial de Pontevedra de 7 de abril de 2017, núm. 166/2017 (accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8031891&links=&optimize=20170525&publicinterface=true. Último acceso: 08.08.2018).

[604] Sentencia de la Audiencia Provincial de Málaga de 16 de septiembre de 2016, núm. 296/2016, FD III (http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7884984&links=&optimize=20161207&publicinterface=true. Último acceso: 08.08.2018) o Sentencia de la Audiencia Provincial de Cantabria de 27 de abril de 2015, núm. 83/2015, FD IV (accesible en:http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7413128&links=&optimize=20150622&publicinterface=true. Último acceso: 08.08.2018).

[605] *"El empresario pondrá en conocimiento de este de una manera clara y destacada, y justo antes de que efectúe el pedido, la información establecida en el artículo 97.1.a), e), p) y q)"*.

En resumen, se pretende que el profesional o empresario que ofrece el servicio de computación en la nube, a través de cláusulas predispuestas que, habitualmente, se establecen para una pluralidad de contratos sin posibilidad de negociación, redacte unas cláusulas lo suficientemente fáciles de conocer por el consumidor, impidiendo utilizar un lenguaje vago o impreciso, facilitando un lenguaje claro y suficientemente detallado, de forma ordenada y sin recurrir en exceso a remisiones, o a un lenguaje particularmente técnico que exijan la colaboración de terceros. Decíamos que los contratos informáticos, entre ellos del *cloud*, requieren de especificaciones técnicas, sobre todo en sus Acuerdos de Niveles de Servicio, que determinan los requerimientos del servicio. Por lo tanto, se requiere una interpretación equilibrada de los requisitos de incorporación de las cláusulas predispuestas y las cláusulas que, por razón del objeto, son necesariamente técnicas para regular la contratación de la nube.

El requisito de la cognoscibilidad pretende que el cliente, en nuestro estudio un consumidor, conozca el contenido del contrato por su puesta a disposición por el proveedor del servicio. Antes de pasar a analizar el requisito, incidir, nuevamente, que la LSSICE exige para la contratación por medios electrónicos, prototipo de la contratación de la nube, que con carácter previo al procedimiento de contratación ponga a disposición del cliente las condiciones del contrato.

La utilización de los medios electrónicos para la contratación del servicio en la nube nos lleva a pensar que, en la gran mayoría de los supuestos, más si cabe cuando el cliente es un consumidor, el contrato principalmente se formalizará por escrito. Es el presupuesto habitual que la LCGC establece en el artículo 5. Teniendo presente el principio de equivalencia funcional, artículo 23.3 de la LSSICE y artículo 3.4 de la Ley de firma electrónica[606], ya tratado en otros capítulos, la exigencia de que el contrato sea por escrito para considerarlo válido aparece, para los contratos a distancia, en el artículo 98.7 del TRLCU. El artículo 5.1 exige que el cliente acepte las condiciones generales de contratación y firme el contrato, que el proveedor informe al cliente de forma expresa de la existencia de las condiciones generales y que le facilite un ejemplar. De este triple requerimiento se desprende algo que es habitual en la contratación de la nube, las condiciones generales de contratación pueden no firmarse con el contrato, sino que el

[606] Ley 59/2003, de 19 de diciembre, de firma electrónica. Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399. Último acceso: 08.08.2018.

proveedor facilitará o indicará dónde se encuentran para que, el cliente, pueda aceptarlas[607]. Esta exigencia de firma del contrato no aparece en el artículo 80.1.a) del TRLCU, sí la facilitación previa o simultánea al contrato de las condiciones generales de contratación no negociadas, *"sin reenvíos a textos o documentos que no se faciliten"*, en el propio contrato o en documentos adjuntos.

El artículo 80.1.b) del TRLCU, además de aludir al requisito de la comprensibilidad, también establece la exigencia de la cognoscibilidad de las cláusulas predispuestas para los contratos celebrados con consumidores. Exige, por tanto, que sean accesibles *"de forma que permita al consumidor y usuario el conocimiento previo a la celebración del contrato sobre su existencia y contenido"*.

Analizados los requisitos para considerar válidas las condiciones generales de contratación y las cláusulas predispuestas, queda por determinar el efecto jurídico de las cláusulas que no reúnan las preceptivas exigencias. PAGADOR LÓPEZ[608] señala que *"el requisito de perceptibilidad y comprensibilidad es un elemento de control (y no de mera interpretación). ... impone al predisponente de cargas o deberes que operan en la fase de formulación o preredacción del clausulado contractual..."*. Las consecuencias del carácter abusivo de las cláusulas predispuestas en los contratos de *cloud computing* parten de la exigencia contenida en el artículo 6 de la Directiva 93/13/CEE. El artículo 83 del TRLCU acoge, en nuestro ordenamiento, la no vinculación del consumidor a las cláusulas abusivas contenidas en el contrato[609]. La consecuencia jurídica del incumplimiento de los requisitos de incorporación establecidos para las condiciones generales de contratación, definidos anteriormente y recogidos en el artículo 5 de la LCGC, será la no incorporación del contenido contractual, artículo 7 de la LCGC.

---

[607] No imaginamos, actualmente, un servicio de la nube que no requiera un contrato formalizado por escrito. En el supuesto de que no se formalice, según el artículo 5.3 de la LCGC, solo es necesario que el proveedor del servicio *"garantice al adherente una posibilidad efectiva de conocer su existencia y contenido en el momento de la celebración"*. Es decir, como máximo en el momento de la contratación el cliente debe conocer de manera efectiva las condiciones generales por las que se regirá.

[608] PAGADOR LÓPEZ, Javier: "Requisitos de incorporación de las condiciones generales", *Condiciones Generales de la Contratación y Cláusulas Abusivas,* 2000, Lex Nova, p. 233.

[609] CARBALLO FIDALGO, Marta: "Consecuencias negociales del carácter abusivo de una cláusula. La nulidad parcial del contrato", *La protección del consumidor frente a las cláusulas no negociadas individualmente,* 2013, Bosch, p.199.

Ahondando en el contenido regulatorio, la nulidad de pleno derecho y la no incorporación de las cláusulas afectadas de abusividad o falta de transparencia, según el TRLCU o la LCGC respectivamente, tienen la misma consecuencia funcional, la no incorporación de la cláusula y la conservación del contrato en los términos pactados. No exige, por tanto, la voluntad de las partes contractuales para la continuidad del contrato, salvo que no pudiera subsistir sin tales cláusulas, artículo 10.1 de la LCGC y 83 del TRLCU, que daría lugar a la nulidad total del contrato. CARBALLO FIDALGO[610] argumenta que *"la nulidad parcial preserva el interés contractual del consumidor y condena al empresario a ejecutar el proyecto contractual depurado de enojosas ventajas y reconducido a las exigencias de la buena fe"*. Protección, debe añadir, que puede desvirtuar la voluntad inicial del proveedor de servicios de la nube, si bien, carga la obligación de actuar de buena fe y transparente en el proceder contractual para garantizar un marco regulatorio, entre cliente y proveedor, equilibrado.

Como anteriormente hemos indicado, los artículos 9 y 10 de la LCGC y el artículo 83 del TRLCU prevén la continuación del contrato anulando solo la cláusula abusiva o no transparente. Por lo tanto, si un contrato de la nube establece cláusulas condenatorias, es decir, impone la nulidad del contrato íntegro, estas no se deberán aplicar por contravenir la imperatividad de los textos legales. La mayoría de los autores[611], incluso, defienden la nulidad de las cláusulas salvatorias, alcance hasta el límite legal, por una actuación del proveedor con mala fe y poco transparente con el cliente. Solo, excepcionalmente, en el supuesto de que el contrato no pudiera subsistir sin las cláusulas abusivas o contrarias a la regulación de las condiciones generales, la nulidad será total. De esta forma, la anulación debe tener una entidad suficiente, provocando un desequilibrio manifiesto entre las partes, sin posibilidad de reconstruir de forma equitativa las prestaciones y contraprestaciones.

---

[610] CARBALLO FIDALGO, Marta: "Consecuencias negociales del carácter abusivo de una cláusula. La nulidad parcial del contrato", *La protección del consumidor frente a las cláusulas no negociadas individualmente,* 2013, Bosch, p.200.

[611] Entre otros, PAGADOR LÓPEZ, Javier: "Condiciones generales y cláusulas abusivas", *La defensa de los consumidores y usuarios (comentario sistemático del Texto Refundido aprobado por Real Decreto Legislativo 1/2007)*, 2011, Iustel, p. 1439; y CARBALLO FIDALGO, Marta: "Consecuencias negociales del carácter abusivo de una cláusula. La nulidad parcial del contrato", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch, p.202.

Una segunda opción, la aplicación residual de la ineficacia global del contrato, se regula en el artículo 9 de la LCGC. De esta forma, se *"declarará la nulidad del propio contrato cuando la nulidad de aquellas o su no incorporación afectara a uno de los elementos esenciales del mismo en los términos del artículo 1261 del Código Civil"*, es decir, cuando afecte de forma esencial al objeto o a la causa del contrato.

c. Análisis de las cláusulas contractuales en la prestación del cloud cuando el cliente es un consumidor.

La protección al consumidor del *cloud* se reglamenta en dos momentos: *ex ante* del contrato, a través de un nivel de información previo para dar lugar a un consentimiento informado, y una protección *ex post* para reparar las cláusulas abusivas, desequilibradas o poco transparentes. La regulación establecida en el TRLCU y la LCGC, así como en la normativa europea, se centran en este segundo estadio.

i. Protección al consumidor de la nube antes de la perfección del contrato.

La Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior[612] y la Directiva 2006/114/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, sobre publicidad engañosa y publicidad comparativa[613] exigieron la promulgación, entre otras, de Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores y usuarios[614], afectando y modificando la Ley 3/1991, de 10 de enero, de Competencia Desleal[615] (LCD). Los proveedores de la nube en su práctica comercial deberán cumplir con los términos que establecen los cuerpos legales señalados.

[612] Accesible en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32005L0029. Último acceso: 08.08.2018.

[613] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32006L0114. Último acceso: 08.08.2018.

[614] Accesible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2009-21162. Último acceso: 08.08.2018.

[615] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-1991-628. Último acceso: 08.08.2018.

Respecto a los consumidores, el artículo 4 de la LCD establece que el comportamiento del empresario o profesional se considerará desleal cuando sea *"contrario a las exigencias de la buena fe, el comportamiento de un empresario o profesional contrario a la diligencia profesional"* de manera *"que distorsione o pueda distorsionar de manera significativa el comportamiento económico del consumidor medio o del miembro medio del grupo destinatario de la práctica, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores"*. Esta definición de actos de competencias desleal debe completarse con los actos de engaños, delimitados en el artículo 5 de la LCD, y con el Anexo I establecido en la Directiva 2005/29/CEE, prácticas comerciales que se consideraran desleales en cualquier circunstancia.

Hemos expuesto de manera reiterada que los proveedores de la nube no informan adecuadamente, en la mayoría de los casos, del correcto desarrollo del servicio. La subcontratación, por ejemplo, no suele comunicarse de manera detallada, bien por cuestiones relacionadas con el modelo de negocio, bien por motivos de seguridad. Sin embargo, es una información relevante que debe valorar el consumidor potencial. Por este motivo, será aplicable el artículo 5.1.b de la LCD[616] como práctica desleal, al no aludirse de manera detallada la composición, procedimiento, el origen geográfico, las características esenciales y/o sus especificaciones en la oferta. Si no se informara de esta circunstancia, sería aplicable el artículo 7 de la LCD como omisión engañosa. No solo en la subcontratación es potencialmente aplicable la protección de la omisión engañosa ante una práctica desleal del proveedor. Cuando este proporcione información *"poco clara, ininteligible, ambigua, no se ofrece en el momento adecuado, o no se da a conocer el propósito comercial"* tendrá similar consecuencia jurídica. Ya decíamos que el modelo de negocio de los proveedores que ofrecen servicios de la nube sin coste económico se podría basar en, entre otros, la utilización de la experiencia de los usuarios para otros servicios de la empresa o como canal para realizar actividades de agentes publicitarios. Estas "intenciones" pueden no ser conocidas o, cuanto menos, no suelen transmitirse al consumidor de manera clara.

[616] Es acto de engaño cualquier conducta que contenga información que induzca o pueda inducir a error al cliente siempre que incida en, artículo 5.1.b de la LCD: *"Las características principales del bien o servicio, tales como su disponibilidad, sus beneficios, sus riesgos, su ejecución, su composición, sus accesorios, el procedimiento y la fecha de su fabricación o suministro, su entrega, su carácter apropiado, su utilización, su cantidad, sus especificaciones, su origen geográfico o comercial o los resultados que pueden esperarse de su utilización, o los resultados y características esenciales de las pruebas o controles efectuados al bien o servicio"*.

Para los consumidores, además, se establecen medidas protectoras contra las prácticas engañosas del proveedor de la nube, artículo 21 de la LCD, vinculadas a los códigos de conductas y los diferentes refrendos de organismos de acreditación, común cuando se contrata a través de medios informáticos y, más relevante aún, cuando el pago es a través de las plataformas webs habilitadas; así como a las prácticas comerciales encubiertas, artículo 26 LCD, llevadas a cabo por las empresas de *cloud* con la excusa de informar al cliente de productos acordes con sus necesidades o requerimientos.

El TRLCU principalmente protege a los consumidores una vez celebrado el contrato o en fase de formación. Sin embargo, la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores establece una serie de requisitos necesarios de información al consumidor en los contratos a distancia. Es decir, antes de ser obligado el consumidor, de manera clara y comprensible, el proveedor de la nube debe dar a conocer, entre otros, la existencia de códigos de conducta, si el proveedor actúa en nombre propio, la dirección geográfica, la duración del contrato de la nube, las condiciones de la resolución del contrato y, aspecto muy importante en el *cloud*, la interoperabilidad. El artículo 97 del TRLCU replica el contenido de la Directiva, haciendo una trasposición directa. Su aplicabilidad en la computación en la nube está garantizara al recoger dentro de su ámbito de aplicación a los contratos de *"contenido digital que no se preste en un soporte material"*[617]. Estas exigencias deben completarse con los requisitos formales, artículo 98 del TRLCU, exigidos para los contratos de la nube que se realizan a distancia. Es decir, la propuesta de contratación debe facilitarse en un soporte duradero legible, empleando términos de forma clara y comprensibles, y en castellano, cuanto menos, los requisitos precontractuales. El texto legal, en un afán proteccionista, añade, nuevamente, la exigencia de confirmar al consumidor la efectiva contratación y obliga a facilitar la información precontractual, salvo que ya se hubiere cumplido con la carga en un período anterior a la efectiva contratación y mediando un soporte duradero. Importante es, para el caso de la contratación de un servicio informático, el deber de comunicar de forma

[617] El artículo 59.1.i del TRLCU define "contenido digital" como *"los datos producidos y suministrados en formato digital"*. Más completa es la definición recogida en la Directiva 2011/83/UE, considerando 19. Debe entenderse, a luz de la Directiva, por contenido digital *"los datos producidos y suministrados en formato digital, como programas, aplicaciones, juegos, música, vídeos o textos informáticos independientemente de si se accede a ellos a través de descarga o emisión en tiempo real, de un soporte material o por otros medios. Los contratos de suministro de contenido digital deben incluirse en el ámbito de aplicación de la presente Directiva"*.

anticipada *"el derecho de desistimiento, la duración del contrato, y, en el caso de contratos de duración indefinida, las condiciones de resolución"* (artículo 98.4 del TRLCU). Requisitos formales que se replican en el TRLCU para los contratos celebrados fuera del establecimiento mercantil, como suele ser habitual en la contratación de la nube.

Este esbozo debe completarse con la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior y su trasposición en el Derecho interno a través de Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE), y el cuadro de protección de los consumidores.

HERNÁNDEZ JIMÉNEZ-CASQUET[618] disecciona la compatibilidad de la Directiva de comercio electrónico y el Derecho comunitario con las normas nacionales de protección de los consumidores, estableciendo un marco protector para los consumidores en la contratación electrónica.

- La Directiva 2000/31/CE y la LSSICE, conforme a los artículos 1.3 y 1.2 respectivamente, se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito coordinado que tengan como finalidad la protección de los intereses de los consumidores y usuarios.
- El principio básico que recoge la norma es el consentimiento informado por el consumidor. GARCÍA MEXÍA[619] establece que el elemento preponderante de todo contrato es el consentimiento, es decir, la concurrencia de la oferta y la aceptación entre las partes, más si cabe ante la ausencia física de las partes, que dificulta mucho ponderar si las partes contratantes están de acuerdo en asumir las obligaciones resultantes ante un contrato de *cloud*. Esto requiere que con carácter precontractual se le facilite al consumidor información de manera clara, accesible y transparente, requisitos que no muchas veces se cumplen por los proveedores de la nube, que ocultan las condiciones generales o los términos y condiciones a través de diferentes enlaces, requiriendo por parte del usuario una pericia en la búsqueda.

[618] HERNÁNDEZ JIMÉNEZ-CASQUET, Fernando: "El marco jurídico del comercio y la contratación electrónicos", *Principios de Derecho de internet*, Tirant lo Blanch, 2005, p. 450-453.

[619] GARCÍA MEXÍA, Pablo: "El comercio electrónico. La regulación de contenidos", *Derecho europeo de internet. Hacia la autonomía académica y la globalidad geográfica*, Netbiblo, 2009, p. 240-242.

Diferentes normas sectoriales en el ámbito de ordenación comercial vienen a establecer algunos deberes de información por parte de los proveedores. Ciñéndonos a la regulación de la LSSICE, el artículo 27 traspone las exigencias recogidas en el artículo 10 de la Directiva, son requisitos previos de información la comunicación de forma permanente, fácil y gratuita, de forma clara, comprensible e inequívoca sobre los distintos trámites que deben seguirse para celebrar el contrato; el prestador debe indicar si va a archivar el documento electrónico en el que se formalice el contrato y si este va a ser accesible; debe mostrar los medios técnicos que pone a su disposición para identificar y corregir los errores en la introducción de los datos; y la lengua o lenguas en las que puede formalizarse el contrato. Además, establece como requisito objetivo adicional, la cesión de información sobre los códigos de conducta a los que el prestador de servicios se acogerá, así como la manera de consultar electrónicamente dichos códigos. Estos deberes se establecen como irrenunciables cuando el destinatario del servicio del *cloud* es un consumidor o usuario.

- El artículo 28.3.a de la LSSICE establece como irrenunciables, cuando una de las partes tenga la consideración de consumidor, la confirmación de la recepción de la aceptación de la oferta. CRUZ RIVERO[620] argumenta que la exigencia de la LSSICE en indicar el archivo de la confirmación al consumidor debe interpretarse *"de modo que quede claro que una persona no experta en el funcionamiento del software de exploración de internet que es posible almacenar dicho acuse de recibo, bien mediante la impresión del documento, bien en un archivo electrónico"*, de modo que, *"no tendría sentido esta disposición, si no es para obligar al vendedor a facilitar el almacenamiento de la confirmación efectuada mediante la introducción de un aviso y de un "botón" de imprimir o guardar"*.

Las obligaciones impuestas al proveedor del *cloud*, requisitos a cumplir de manera previa a la correcta formalización del contrato, en gran medida son coincidentes en los diferentes cuerpos normativos reseñados. Baste repasar la información previa impuesta por el TRLCU, estudiada *ad supra*.

[620] CRUZ RIVERO, Diego: "Contratación electrónica con consumidores", *Revista de Contratación Electrónica*, 2009, nº 109, p. 21.

ii. Ámbito de aplicación

Uno de los principales problemas que nos encontramos en la aplicabilidad de las normas garantistas para con los consumidores es su ámbito de aplicación. Para la contratación de la nube solemos utilizar medios electrónicos o informáticos, contratamos con proveedores que, por la concentración de grandes cuotas de mercado, no suelen estar radicados en territorio nacional, y se utiliza un *hardware* por los prestadores del servicio que, por razones de costes, se suelen ubicar en terceros países. Aunque el cliente puede ser previsor, pudiendo estudiar y analizar los problemas que estas circunstancias generan en su relación contractual, difícilmente podrá alterar de forma relevante su poder negociador. Consecuentemente, es necesario determinar el ámbito de aplicación de las normas nacionales referentes a la protección del consumidor, no solo para una protección precontractual, ya estudiada, también para la viabilidad de las cláusulas predispuestas o condiciones generales del servicio de la nube. En palabras de GARCÍA MEXÍA[621], *"la necesidad de salvaguardar con especial cuidado el status del consumidor en la sociedad de la información, tiene también su proyección en el ámbito de la jurisdicción, y de la ley en su caso aplicable a las relaciones jurídicas en que aquél intervenga"*. La finalidad no es otra que la de facilitar al consumidor la defensa de los derechos e intereses que le corresponden, evitando que el consumidor tenga que acudir a soluciones judiciales especialmente gravosas. De esta forma, en la determinación del foro competente y de la ley aplicable se estará a lo dispuesto en las normas de Derecho Internacional Privado.

Tratando en primer lugar la competencia judicial, regulada actualmente por el Reglamento (UE) nº 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, Bruselas I bis, la competencia, como regla general, recaerá en los órganos jurisdiccionales del Estado miembro donde se encuentren domiciliadas las personas, independientemente de su nacionalidad, artículo 4. Sin embargo, como ya sea puesto de manifiesto, en el contrato de la computación en la nube raramente encontraremos que las partes en conflicto estén domiciliadas en España.

Partiendo del fundamento jurídico establecido en el artículo 18.1 del Reglamento, cuando el consumidor de la nube demande al prestador del servicio podrá optar por

[621] GARCÍA MEXÍA, Pablo: "El comercio electrónico. La regulación de contenidos", *Derecho europeo de internet. Hacia la autonomía académica y la globalidad geográfica*, Netbiblo, 2009, p. 255.

interponer la acción ante los órganos jurisdiccionales del Estado miembro en que estuviere domiciliada dicha parte o, *"con independencia del domicilio de la otra parte, ante el órgano jurisdiccional del lugar en que esté domiciliado el consumidor"*. Bruselas I bis aclara la norma que le precede[622], declarando, expresamente, que es indiferente el domicilio del proveedor de la nube. El consumidor, en la mayoría de los supuestos, optará por los juzgados y tribunales de su Estado, por conocimiento y costes. Sin embargo, cuando es el proveedor quien entabla acción contra el consumidor solo podrá *"interponerse ante los órganos jurisdiccionales del Estado miembro en que esté domiciliado el consumidor"*, artículo 18.2.

La regulación debe completarse con el artículo 19. Las cláusulas de sumisión a los juzgados y tribunales de un Estado miembro distinto de las partes, cuando una de las partes sea consumidor, no producirán efectos siempre que aquellos tengan la consideración de consumidores pasivos. En consecuencia, habrá que determinar qué se considera consumidor pasivo. Es consumidor pasivo, a tenor del citado Reglamento, el consumidor captado en su propio mercado, es decir, cuando el empresario o profesional, por cualquier medio, dirigiera sus actividades comerciales o profesionales al Estado miembro del domicilio del consumidor o de varios Estados miembros (artículo 17.1.c)[623]. En este supuesto, las cláusulas de los contratos de *cloud* que determinen la sumisión a tribunales no producirán efectos[624].

---

[622] Reglamento (CE) nº 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Accesible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2001-80073. Último acceso: 08.08.2018.

[623] Sin querer ahondar en exceso qué acciones comerciales podemos considerarlas dirigidas hacia los consumidores de otros Estados miembros, la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 7 de diciembre de 2010, en los asuntos acumulados Peter Pammer contra Reederei Karl Schlüter GmbH & Co. KG (C-585/08) y Hotel Alpenhof GesmbH contra Oliver Heller (C-144/09), estableció como indicios para determinar que la actividad está dirigida hacia un vendedor cuando la actividad tenga carácter internacional, se utilice una lengua o una divisa distinta de la habitualmente empleada en el Estado miembro en el que esté establecido el vendedor, se mencione números de teléfonos con prefijos internacionales o se utilice un nombre de dominio de primer nivel distinto al del estado miembro en que está establecido el vendedor, entre otros. Muchos de estos indicios aparecen en las relaciones contractuales establecidas entre los proveedores de *cloud* y los consumidores españoles.
Accesible en: http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0585&lang1=es&type=NOT&ancre. Último acceso: 08.08.2018.

[624] La admisibilidad y la forma de la elección del foro en el contrato con consumidores se desarrollará en el estudio pormenorizado de las cláusulas del contrato del *cloud* con consumidores, desarrollado en el siguiente subapartado.

Cuando el proveedor de servicios de *cloud* esté domiciliado fuera de la Unión Europea, habrá que atenerse a la regulación establecida en el artículo 22.4 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial[625]. Este precepto establece la competencia a los Tribunales españoles cuando la celebración del contrato hubiere sido precedida por una oferta personal o por publicidad realizada en España; así cuando el consumidor hubiere llevado a cabo en territorio español los actos necesarios para la celebración del contrato. Por lo tanto, y como consecuencia de dicha alternatividad, los Tribunales españoles serán competentes para conocer toda contratación de servicios de *cloud* realizada de manera online, aunque el proveedor no se dirija directamente hacia el mercado español.

El Reglamento (CE) nº 593/2008 del Parlamento europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales[626], Roma I, establece la norma de conflicto para la resolución de los contratos de la nube. Cuando una de las partes del contrato sea un consumidor[627], el artículo 6.2 del citado Reglamento establece las dos premisas básicas aplicables a un contrato de consumo. En primer lugar, la elección de la ley aplicable, elegida por las partes, no privará al consumidor de la protección de la ley imperativa del país de su residencia habitual. Es decir, al consumidor le serán aplicables todas las normativas tuitivas de los consumidores del ordenamiento jurídico donde tiene su residencia habitual. Como señala ÁLVAREZ DE SOTOMAYOR[628], *"la contratación con participación de consumidores deben ser respetadas, por lo que el régimen jurídico del contrato internacional será el resultado de combinar la ley del contrato elegida válidamente por las partes con las normas imperativas aplicables a los*

---

[625] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666. Último acceso: 08.08.2018.

[626] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32008R0593. Último acceso: 08.08.2018.

[627] Artículo 6.1: *"Sin perjuicio de los artículos 5 y 7, el contrato celebrado por una persona física para un uso que pueda considerarse ajeno a su actividad comercial o profesional («el consumidor») con otra persona («el profesional») que actúe en ejercicio de su actividad comercial o profesional, se regirá por la ley del país en que el consumidor tenga su residencia habitual, siempre que el profesional: a) ejerza sus actividades comerciales o profesionales en el país donde el consumidor tenga su residencia habitual, o b)por cualquier medio dirija estas actividades a ese país o a distintos países, incluido ese país, y el contrato estuviera comprendido en el ámbito de dichas actividades"*.

[628] ÁLVAREZ DE SOTOMAYOR, Silvia Feliu: "Nulidad de las cláusulas de jurisdicción y ley aplicable a la luz de la Ley 3/2014 por la que se modifica el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios", *Revista electrónica de estudios internacionales (REEI)*, 2015, nº 29, p. 9. Accesible en: http://www.reei.org/index.php/revista/num29/archivos/Estudio_FELIU_Silvia.pdf. Último acceso: 28.08.2017.

aspectos concretos del ordenamiento jurídico del Estado donde el consumidor resida habitualmente". En segundo lugar, sin perjuicio de cumplir con los requisitos establecidos en los artículos 5 y 7 y de las propias características que establece el precepto regulador, el contrato de *cloud* se regirá por la ley del país en el que el consumidor tenga su residencia habitual siempre que el proveedor ejerza su actividad en el país en el que tenga residencia habitual el consumidor o dirija actividades tendentes a la contratación en ese país. Por lo tanto, vuelve a presentarse la noción de consumidor pasivo.

En resumen, cabría la elección de ley aplicable pero no produciría efectos derogatorios de las normas imperativas de protección del consumidor pasivo (aquellas de su lugar de residencia, que en el caso del consumidor español se concretan, principalmente, en los preceptos del TRLCU). Se ha de añadir que el artículo 11.4 del Reglamento[629] determina la ley aplicable a los contratos de consumo, siendo esta la del país en el que tenga residencia habitual el consumidor.

iii. Protección ex post, estudio de las cláusulas contractuales en la contratación con consumidores.

En el apartado .a del presente capítulo hemos tratado las condiciones generales y las cláusulas específicas en el contrato de *cloud computing* sobre la base de una relación entre empresas. En este estudio de la protección al consumidor *ex post*, ahondaremos en las cláusulas del contrato de la nube que pueden entrar en conflicto con la protección de los consumidores y usuarios. Para lo no tratado en el presente apartado, es plenamente aplicable lo expuesto en el estudio de la relación B2B.

a. Protección de datos

En el Capítulo IV.b se ha realizado un estudio completo a la adecuación de la normativa aplicable en protección de datos personales, debiendo ser reproducidas las conclusiones realizadas[630].

---

[629] *"La forma de estos contratos se regirá por la ley del país en que tenga su residencia habitual el consumidor"*.

[630] En el presente estudio nos centraremos, exclusivamente, en su adecuación al TRLCU. De igual forma, se analizará la protección de datos con alcance genérico, no exclusivamente de los datos de carácter personal. En próximos subapartados se tratará del tratamiento y localización de datos.

En el presente traemos a colación la responsabilidad de los proveedores de la nube por la integridad de los datos proporcionados en el servicio, así como la integridad de los datos de los clientes. Independientemente de que el servicio tenga o no un coste económico, los proveedores de servicio suelen limitar su responsabilidad por la pérdida o acceso a los datos, ciñéndose a la débil obligación de realizar un cuidado razonable en función de sus capacidades.

En la razón de ser de la prestación del servicio está que el cliente pueda asegurar, y por lo tanto será responsabilidad del proveedor, un cierto grado de integridad y confidencialidad en los datos que aportan al servicio. La dificultad de delimitar la responsabilidad se agrava, como ya expusiéramos, cuando el prestador del servicio se sirve de otras empresas para efectuar parte de la prestación. En aras de la transparencia y la correcta relación entre partes, el prestador principal debe comunicar al cliente, como una de las obligaciones *ex ante*, las entidades implicadas en la correcta realización del servicio y las medidas que garantizan la confidencialidad y la integridad de los datos expuestos en el desarrollo de la nube.

HOSTALIA, que dispone de servidores *cloud*, recoge en los TÉRMINOS Y CONDICIONES DEL CONTRATO[631] que *"declina cualquier responsabilidad sobre la vulneración de los sistemas de seguridad del Cliente o de la inviolabilidad de los datos de carácter personal cuando estos son transportados a través de cualesquiera redes de telecomunicación"*. A pesar de esta exención de responsabilidad general, sí acepta, dentro del CONTRATO DE TRATAMIENTO DE DATOS[632], que *"acens se compromete a mantener el secreto profesional respecto de los Datos de Carácter Personal y al deber de guardarlo, obligación que subsistirá aún después de finalizar la relación contractual con la Compañía"*. Más claro resulta DROPBOX[633] al indicar que *"solo seremos responsables por las pérdidas y daños que sean un resultado razonablemente previsible*

[631] TÉRMINOS Y CONDICIONES DEL CONTRATO de HOSTALIA, versión de 08.08.2018. Accesible en: https://www.hostalia.com/contratar/contrato/. Último acceso: 08.08.2018.

[632] CONTRATO DE TRATAMIENTO DE DATOS PARA SERVICIOS DE ALOJAMIENTO DE ACENS (HOSTALIA es una empresa del grupo ACENS, siguiendo los patrones y la reglamentación establecida para la empresa principal), versión de 08.08.2018. Accesible en: https://www.acens.com/file_download/contrato_tratamiento_de_datos_personales.pdf. Último acceso: 08.08.2018.

[633] CONDICIONES DE SERVICIO DE DROPBOX, versión 17.04.2018. Accesible en: https://www.dropbox.com/privacy#terms. Último acceso: 08.08.2018.

de nuestro fallo a la hora de prestar un cuidado y una actuación razonablemente competente, así como algún incumplimiento de nuestro contrato contigo", añadiendo que *"no afecta a los derechos del consumidor irrenunciables o que no se puedan limitar por medio de ningún contrato o acuerdo"*.

Un supuesto extremo podemos encontrarlo con la contratación del *cloud* de BOX. En sus TÉRMINOS DE SERVICIO[634] responsabiliza de manera directa al cliente, al determinar que *"es su responsabilidad* (cliente) *configurar y utilizar en forma adecuada el Servicio y las Zonas de Box correspondientes para cumplir con sus obligaciones relacionadas con los tipos de datos y las obligaciones de residencia de datos"*.

Como puede observarse, pocos prestadores del servicio formulan la protección de datos en sentido genérico, es decir, no específicamente sobre los datos de carácter personal.

Dentro de las determinadas cláusulas negras en el control de validez de las cláusulas no negociadas[635] se encuentran, en el artículo 85.7 del TRLCU, las cláusulas que supongan la supeditación a una condición cuya realización depende únicamente de la voluntad del empresario para el cumplimiento de las prestaciones, cuando al consumidor se le haya exigido un compromiso firme. Qué duda cabe que debe ser el prestador del servicio quien facilite las medidas de seguridad oportunas para la correcta protección de los datos, por lo tanto, hacer recaer en el comportamiento del consumidor la correcta integridad y confidencialidad de los datos supone una cláusula abusiva. Por supuesto, el cliente debe realizar un uso aceptable del servicio que no exponga a riesgos desproporcionado los datos y la información suministrada, debiendo imponerse un equilibrio de actuaciones en función de las correctas capacidades. El artículo 85.7 prescribe *"genéricamente cualquier fórmula que permita el sometimiento a la voluntad del empresario de la ejecución de las prestaciones que le gravan, estén o no definidas"*.

---

634 TÉRMINOS DE SERVICIO DE BOX, vigente desde 01.08.2017. Accesible en: https://www.box.com/es-419/legal/termsofservice. Último acceso: 18.11.2017.

635 CARRASCO PERERA, Ángel: "Control de validez de condiciones generales y cláusulas abusivas", *Derechos de contratos,* 2017, Aranzadi. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

b. Variación de los términos del contrato

A lo largo de nuestro estudio de las cláusulas contractuales de la nube hemos mencionado que el servicio, en su desarrollo, puede encontrarse con cambios en su configuración, indispensables para el buen funcionamiento de los sistemas de información. Los proveedores pueden hacer referencia a tales cambios en el ANS, pero en otras ocasiones pueden establecerse cláusulas generales de variación de los términos del contrato o, simplemente, no hacer mención de la posibilidad futura.

Las cláusulas que de modo genérico faculten al proveedor de servicio a la modificación unilateral del contrato serán consideradas abusivas, artículo 85.3 del TRLCU[636], salvo que *"concurran motivos válidos especificados en el contrato"*. En consecuencia, siguiendo el artículo 1.256 CC, si el prestador de los servicios del *cloud* predispone la posibilidad de modificar unilateralmente las condiciones establecidas para el servicio, la cláusula debe considerarse abusiva. La normativa española no distingue, como sí lo hace la Directiva de aplicación, entre la modificación de los términos del contrato o la modificación por el empresario de los servicios a suministrar[637], debiendo ser comprendidas ambas circunstancias en el artículo 85.3. La excepción establecida, es decir, la justificación de la modificación del clausulado por el empresario o profesional debe equivaler a una causa objetiva, como puede ser una mejora en la seguridad del servicio, siempre que, como señala la doctrina[638], no atienda exclusivamente a una mejora en el rendimiento económico del empresario y el perjuicio de la medida no repercuta o lesione al consumidor. CUNNINGHAM y REED [639] consideran, incluso, que aunque los

---

[636] *"Las cláusulas que reserven a favor del empresario facultades de interpretación o modificación unilateral del contrato, salvo, en este último caso, que concurran motivos válidos especificados en el contrato"*.

[637] Directiva 93/13/CEE, anexo 1.j) (*"Autorizar al profesional a modificar unilateralmente sin motivos válidos especificados en el contrato los términos del mismo"*) y anexo 1.k) (*"Autorizar al profesional a modificar unilateralmente sin motivos válidos cualesquiera características del producto que ha de suministrar o del servicio por prestar"*). Hace referencia a las cláusulas que pueden ser consideradas abusivas.

[638] Entre otros: CARBALLO FIDALGO, Marta: "Las cláusulas en todo caso prohibidas (II)", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch, p. 134; y FERRER RIBA, Josep: "Disposición Adicional Primera. Seis. 2ª", *Comentarios a la Ley sobre Condiciones Generales de Contratación*, 2002, Civitas, p. 1006.

[639] CUNNINGHAM, Alan; y REED, Chris: "Caveat Consumer? – Consumer Protection and Cloud Computing Part 2 – The Application of ex ante and ex post Consumer Protection Law in the Cloud", *Queen Mary University of London - Legal Studies Research Paper*, 2013, nº 133, p. 33. Accesible en: https://ssrn.com/abstract=2212051. Último acceso: 08.08.2018.

requisitos técnicos y logísticos del servicio de la nube pueden requerir una modificación del contrato, la realización de forma unilateral por el proveedor del servicio debe considerarse desproporcionada, incluso ante servicios "gratuitos", siempre que el cliente no sea avisado.

Consideramos que no entra dentro del supuesto anterior la disposición que establece la posibilidad de modificación de las condiciones del contrato por el proveedor de la nube si presta la posibilidad, al cliente, de manifestarse sobre los cambios establecidos en el contrato, siempre que requiera manifestación expresa para determinar la continuidad del servicio reformulado, durante un período de plazo suficiente. Así lo consideraba la Directiva 93/13/CEE, en el Anexo 2.b). 2 párrafo (*"la letra j) se entiende sin perjuicio también de las cláusulas por las que el profesional se reserve el derecho a modificar unilateralmente las condiciones de un contrato de duración indeterminada siempre que el profesional esté en la obligación de informar al consumidor con una antelación razonable, y de que este tenga la facultad de rescindir el contrato"*), disposición que no se ha recogido en el TRLCU de forma genérica, solo para los servicios financieros, artículo 85.3.3 párrafo.

Para ICLOUD de APPLE[640], el proveedor se reserva el derecho a modificar el contrato en cualquier momento, pudiendo establecer nuevas cláusulas, si bien lo condiciona a que *"Apple le notifique con 30 días de antelación cualquier cambio sustancial adverso en el Servicio o en las condiciones de uso aplicables del servicio, a menos que no sea razonable hacerlo por circunstancias derivadas de medidas legales, reglamentarias o gubernamentales; para solucionar los problemas de seguridad del usuario, de privacidad del usuario o de integridad técnica; para evitar interrupciones del servicio para otros usuarios"*. Esta posibilidad de modificación unilateral del proveedor, sea sustancial como en el anterior supuesto o no, no aparece en los servicios de la nube de pago (salvo que concurran las circunstancias anteriores establecidas para la omisión de notificación del cambio sustancial en el servicio gratuito, es decir, las causas para la omisión de la notificación las considera, para la nube de pago, causas de modificación unilateral). Para el servicio gratuito y de pago reconoce el derecho del

[640] TÉRMINOS Y CONDICIONES DE ICLOUD de APPLE, versión de 19.09.2017. Accesible en: https://www.apple.com/legal/internet-services/icloud/es/terms.html. Último acceso: 08.08.2018.

cliente a rescindir el contrato y las condiciones de uso. GOOGLE[641], sin embargo, dispone que será el consumidor quien deba *"revisar las condiciones periódicamente"*, publicando, sin especificar dónde, avisos sobre los mismos. No establece ningún derecho al cliente de rescisión del contrato, simplemente recomienda, en caso de no aceptar las condiciones modificadas, *"cancelar el uso de dicho Servicio"*.

Hemos defendido la aceptación expresa del cliente, además de una notificación sobre los cambios producidos. MICROSOFT[642] añade para sus servicios, entre los que se encuentra la nube ONEDRIVE, la aceptación tácita si continúa con los servicios una vez que entre en vigor las modificaciones notificadas[643]. Carga excesiva que asume el consumidor, más considerando las implicaciones del acto.

Dentro de las modificaciones de las cláusulas del contrato, supuestos particulares pueden considerarse las modificaciones de las tarifas o el cambio de un servicio "gratuito" a oneroso, abusivas según el artículo 85.10 del TRLCU; la prórroga automática del contrato de duración determinada si el consumidor no se manifiesta en contra, y/o fijando una fecha límite de oposición que dificulte manifestar su voluntad, abusivas conforme el artículo 85.2 del TRLCU; la modificación de la duración del contrato, de forma extintiva, en contratos de duración indefinida en un plazo breve, sin notificación razonable; o la resolución discrecional por el proveedor, si esa facultad no se reconoce al consumidor, cláusulas abusivas establecidas en los artículos 85.4 y 87.3 del TRLCU.

Respecto a la modificación unilateral de los precios por el empresario o profesional, el Tribunal de Justicia de la Unión Europea, en la Sentencia de 21 de marzo de 2013, asunto c-92/11[644], considera legítimo el interés del empresario en modificar los precios en los contratos de duración indeterminada, como es habitual en el *cloud*, condicionado al interés legítimo del consumidor de conocer y prever las consecuencias del cambio. Es

---

[641] CONDICIONES DEL SERVICIO DE GOOGLE, versión 25.10.2017 (última versión). Accesible en: https://www.google.com/intl/es-419/policies/terms/. Último acceso: 08.08.2018.

[642] MICROSOFT SERVICES AGREEMENT, publicación de 01.03.2018 (última versión). Accesible en. https://www.microsoft.com/es-es/servicesagreement/. Último acceso: 08.08.2018.

[643] *"Le proporcionaremos la oportunidad de cancelar los Servicios con un mínimo de treinta (30) días antes de que el cambio entre en vigor. El uso de los Servicios después de la entrada en vigor de los cambios implicará su aceptación de los nuevos términos"*.

[644] Accesible en: http://curia.europa.eu/juris/celex.jsf?celex=62011CJ0092&lang1=es&type=TXT&ancre. Último acceso: 08.08.2018.

decir, se imponen las *"las exigencias de buena fe, equilibrio y transparencia"*. Por lo tanto, sería posible que el prestador del servicio de la computación en la nube modifique unilateralmente el contrato siempre que reúna los siguientes principios esenciales: *"por una parte, si en el contrato se expone de manera transparente el motivo y el modo de variación del coste relacionado con el servicio que ha de prestarse, de forma que el consumidor pueda prever, sobre la base de criterios claros y comprensibles, las eventuales modificaciones del coste, y, por otra parte, si el consumidor dispone del derecho a rescindir el contrato en caso de que el coste se modifique efectivamente"*. Esta facultad de rescisión conferida al consumidor no debe ser meramente formal, posibilitando al cliente su ejercicio efectivo. Como señala MENDOZA LOSANA[645], las obligaciones anteriormente anunciadas no exoneran a los proveedores de informar a los clientes de la modificación de la tarifa con suficiente antelación, antes de producirse el hecho, para poder efectuar su derecho de rescisión, ni considerase cumplida la obligación principal de información con una mera remisión a documentos adicionales.

c. Jurisdicción y sumisión al arbitraje

En el estudio de CUNNINGHAN y REED[646] se evidencia, como en el contrato entre empresarios y profesionales, que una de las cláusulas más habituales es aquella que determina el foro y la jurisdicción. Vinculada, generalmente, con la elección de la normativa aplicable, que se estudiará en el próximo subapartado, y la sumisión al arbitraje, pueden propiciar un grave desequilibrio entre partes[647]. CARBALLO

[645] MENDOZA LOSANA, Ana Isabel: "Control de condiciones generales de la contratación en sectores regulados. En particular, la cláusula que permite la modificación unilateral de los precios", *Centro de Estudios de Consumo*, 2013, p. 8. Accesible en: https://ruidera.uclm.es/xmlui/handle/10578/8818. Último acceso: 08.08.2018.

[646] CUNNINGHAM, Alan; y REED, Chris: "Caveat Consumer? – Consumer Protection and Cloud Computing Part 2 – The Application of ex ante and ex post Consumer Protection Law in the Cloud", *Queen Mary University of London - Legal Studies Research Paper*, 2013, nº 133, p. 31. Accesible en: https://ssrn.com/abstract=2212051. Último acceso: 08.08.2018.

[647] Recomendamos el estudio de la Sentencia del Tribunal Supremo de 23 de julio de 1993, n. 5677/1993 (http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2216465&links=&optimize=20040624&publicinterface=true, último acceso: 08.08.2018) y la Sentencia del Tribunal Supremo de 20 de febrero de 1998, núm. 1137/1998 (http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2339589&links=sumisi%C3%B3n%20expresa&optimize=20040521&publicinterface=true, último acceso: 08.08.2018).

FIDALGO[648] estudia cómo la cláusula de sumisión expresa supone una fórmula obstruccionista de acceso a la justicia, obligando a los consumidores a desplazarse a foros desconocidos para organizar su defensa, incrementando la complejidad y el coste económico a favor del proveedor, en nuestro estudio, del *cloud*.

Antes de analizar si materialmente la elección de la jurisdicción en los contratos de la nube contraviene del TRLCU, debe cuestionarse la admisibilidad de la cláusula, aspecto que determina la ley del foro.

En materia de contrato con consumidores, como señaláramos en el aparatado ii), la regulación se encuentra establecida en el Reglamento Bruselas I bis. El artículo 17.1.c del Reglamento establece que la competencia quedará determinada, en los contratos de la nube, *"cuando la otra parte contratante ejerza actividades comerciales o profesionales en el Estado miembro del domicilio del consumidor o, por cualquier medio, dirija tales actividades a dicho Estado miembro o a varios Estados miembros, incluido este último, y el contrato esté comprendido en el marco de dichas actividades"* (definición del concepto de actividad dirigida). Vínculo que se desvirtúa, por una aplicación exorbitante, como se reseñará en el siguiente subapartado, al ser exigible, sin exclusiva, que esa actividad se dirija al territorio de cualquier Estado o Estados del Espacio Económico Europeo.

Los foros se establecen en el artículo 18[649], pudiendo modificarse siempre que el acuerdo o los acuerdos respeten las condiciones de admisibilidad establecidas en el artículo 19. Por lo tanto, los acuerdos de selección del foro, salvo que coincidan con los determinados en el artículo 18, deberán nacer posteriores al litigio, o deberá permitir al consumidor formular demandas ante órganos jurisdiccionales distintos a los indicados en la sección, o bien que *"habiéndose celebrado entre un consumidor y su cocontratante, ambos domiciliados o con residencia habitual en el mismo Estado miembro en el*

[648] CARBALLO FIDALGO, Marta: "Las cláusulas en todo caso prohibidas (II)", *La protección del consumidor frente a las cláusulas no negociadas individualmente"*, 2013, Bosch, p. 193.

[649] Artículo 18: *"1. La acción entablada por un consumidor contra la otra parte contratante podrá interponerse ante los órganos jurisdiccionales del Estado miembro en que esté domiciliada dicha parte o, con independencia del domicilio de la otra parte, ante el órgano jurisdiccional del lugar en que esté domiciliado el consumidor.2. La acción entablada contra el consumidor por la otra parte contratante solo podrá interponerse ante los órganos jurisdiccionales del Estado miembro en que esté domiciliado el consumidor.3. El presente artículo no afectará al derecho de formular una reconvención ante el órgano jurisdiccional que conozca de la demanda inicial de conformidad con la presente sección"*.

momento de la celebración del contrato, atribuyan competencia a los órganos jurisdiccionales de dicho Estado miembro, a no ser que la ley de este prohíba tales acuerdos". Se formula por alternatividad.

La elección del foro estará condicionada al contraste del contenido con los presupuestos establecidos en los artículos 82 a 91 del TRLCU, conforme al artículo 67.2 del TRLCU[650].

Partiendo de la consideración de que es abusiva toda cláusula que contravenga las reglas de la competencia, artículo 82.4.f), es el artículo 90.2 del TRLCU el que establece como abusivo *"la previsión de pactos de sumisión expresa a Juez o Tribunal distinto del que corresponda al domicilio del consumidor y usuario, al lugar del cumplimiento de la obligación o aquél en que se encuentre el bien si este fuera inmueble"*.

SEAGATE, que tiene servicios de datos en nube para "consumidores externos", señala en sus TÉRMINOS Y CONDICIONES[651] que "*cualquier procedimiento legal que surja del uso de este sitio, su contenido o cualquier otro material en él incluido, así como estos términos, se debe interponer en Santa Clara (California) y se debe interponer en el transcurso de un año después del reclamo o de que la causa de acción surja…. Al usar este sitio, el usuario se somete irrevocablemente a la jurisdicción del estado y las cortes federales de Santa Clara (California)"*. Además, introduce una medida contraria a la protección de los consumidores: *"si por alguna razón una corte de jurisdicción competente encuentra alguna que provisión de estos Términos no es aplicable, esa provisión se implementará a la máxima extensión permisible para efectuar el objetivo de estos Términos, y el recordatorio de estos Términos continuará en total fuerza y efecto"*. Las cláusulas salvatorias, como señaláramos en el apartado b), suponen una actuación

---

650 *"Las normas de protección frente a las cláusulas abusivas contenidas en los artículos 82 a 91, ambos inclusive, serán aplicables a los consumidores y usuarios, cualquiera que sea la ley elegida por las partes para regir el contrato, cuando este mantenga una estrecha relación con el territorio de un Estado miembro del Espacio Económico Europeo"*.

651 TÉRMINOS Y CONDICIONES de SEAGATE, última versión 03.08.2015. Accesible en: https://www.seagate.com/es/es/legal-privacy/terms-and-conditions/. Último acceso: 08.08.2018. Nótese que la dirección contempla la clasificación por región, ES-ESPAÑA.

poco transparente y de mala fe respecto al consumidor, debiendo considerarse nula, a priori, por los artículos 9 y 10 de la LCGC y el artículo 83 del TRLCU[652].

En otro orden de cosas, por razón de la materia es práctica común que los proveedores de la nube impongan la cláusula de sumisión al arbitraje para las disputas entre el suministrador y los consumidores. El desequilibrio que se produce entre el profesional del servicio y los consumidores conlleva a la nulidad radical, incluso aunque no sea invocada por el cliente[653]. La Ley 60/2003, de 23 de diciembre, de Arbitraje[654] establece la anulación y revisión del laudo cuando, artículo 41, los árbitros hayan resuelto sobre cuestiones no susceptibles de arbitraje, así *"como la designación de los árbitros o el procedimiento arbitral no se han ajustados al acuerdo entre las partes, salvo que dicho acuerdo fuera contrario a una norma imperativa de esta Ley, o, a falta de dicho acuerdo, que no se han ajustado a esta ley"*. CARRASCO PERERA[655] señala la cláusula de sumisión de arbitraje como cláusula negra en los niveles de control de validez de las cláusulas no negociadas. El artículo 90.1 del TRLCU considera abusiva la sumisión a arbitrajes distintos del arbitraje de consumo, salvo que se trate de órganos de arbitraje institucionales creados por normas legales para un sector o un supuesto específico.

Ya señalamos que ADRIVE en el documento TERMS OF SERVICES[656] establece la cláusula de sumisión del arbitraje, de San Francisco, California, EE.UU., como la única

---

[652] Resulta paradójico que el proveedor declare que "*Seagate no se responsabiliza del grado de adecuación de los materiales de este sitio para el uso en ubicaciones externas a EE. UU. y el acceso a este Sitio desde otros países donde su contenido o uso sea ilegal o esté prohibido"*, sin embargo, se dirija a los clientes potenciales españoles clasificando la información según la procedencia. En la dirección web se recoge el directorio /es/.

[653] Recomendamos la lectura de las Sentencia del Tribunal de Justicia (Sala Primera), de 26 de octubre de 2006, caso Elisa María Mostaza Claro contra Centro Móvil Milenium SL, asunto C-168/05 (accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62005CJ0168) y la Sentencia del Tribunal de Justicia (Sala Quinta), de 21 de noviembre de 2002, caso Cofidis SA contra Jean-Louis Fredout, asunto C-473/00 (accesible en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A62000CJ0473). Últimos accesos: 08.08.2018.

[654] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2003-23646. Último acceso: 08.08.2018.

[655] CARRASCO PERERA, Ángel: "Control de validez de condiciones generales y cláusulas abusivas", *Derechos de contratos,* 2017, Aranzadi. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

[656] Se puede acceder a los TERMS OF SERVICES de ADRIVE en: http://www.adrive.com/terms. Condiciones a fecha de 08.08.2018 (Última actualización: 22.09.2015). Último acceso: 08.08.2018.

forma de resolver la disputa entre partes[657]. La cláusula no discrimina entre clientes. En similares términos se redacta el HUAWEI ID USER AGREEMENT[658], que regula el *cloud* de HUWAI para consumidores, señalando como centro de arbitraje el Hong Kong International Arbitration Centre (HKIAC)[659].

d. Ley aplicable

En la mayoría de los términos y condiciones analizados, los proveedores de los servicios de la nube señalan como legislación aplicable aquella donde reside el prestador del servicio o donde tiene su centro de actividad principal, garantizándose un tratamiento más favorable para su parte. La elección de esta legislación suele imposibilitar a los consumidores defender su posición en los juzgados y tribunales, el desconocimiento de la normativa y los costes asociados son uno de los principales problemas a los que se enfrentan los clientes, agravantes similares al supuesto de elección de la jurisdicción.

ICLOUD de APPLE en sus TÉRMINOS Y CONDICIONES DE ICLOUD[660] establece una diferenciación según la nacionalidad del "ciudadano". En términos generales establece que *"este Contrato y la relación entre usted y Apple se regirán por las leyes del Estado de California en EE.UU., excepto en los casos en que se produzca un conflicto con las disposiciones legales"*, añadiendo que *"si usted (a) no es ciudadano estadounidense; (b) no reside en Estados Unidos; (c) no accede al Servicio desde Estados Unidos; y/o (d) no es ciudadano de ninguno de los países que se indican más adelante, acepta por el presente que cualquier conflicto o reclamación que pueda surgir de este Contrato se regirá por la legislación aplicable, indicada más adelante, independientemente de cualquier conflicto que pueda producirse con las disposiciones*

---

[657] *"Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The arbitration shall be conducted in San Francisco, California, and any judgment on the arbitration award may be entered in any court having jurisdiction thereof"*.

[658] HUAWEI ID USER AGREEMENT, última versión de 01.2018. Accesible en: https://hwid5.vmall.com/CAS/portal/agreements/userAgreement/en-us_userAgreement.html?version=common. Último acceso: 08.08.2018

[659] *"You and Huawei agree that any and all disputes, claims and propositions arising out of performance of this Agreement and acceptance of this Service under this Agreement shall be submitted to the Hong Kong International Arbitration Centre (HKIAC) and shall be governed by the arbitration rules"*.

[660] TÉRMINOS Y CONDICIONES DE ICLOUD de APPLE, versión de 19.09.2017. Accesible en: https://www.apple.com/legal/internet-services/icloud/es/terms.html. Último acceso: 08.08.2018.

legales". Sin embargo, si el cliente es residente en la Unión Europea, Suiza, Noruega o Islandia se regirá por las leyes de su residencia habitual. Es apreciable como el proveedor de servicios intenta imponer, a toda costa, la legislación donde radica su sede central y como, previsiblemente, el marco normativo le obliga a practicar la excepción con los ciudadanos residentes en la Unión Europea. GOOGLE, en sus CONDICIONES DE SERVICIO[661], ni siquiera discrimina entre clientes imponiendo *"las leyes de California, EE.UU., excluyendo los conflictos de leyes de California"* en cualquier controversia que surja "*o se relacione con las presentes condiciones o los Servicios"*.

Una regulación opuesta aparece en el SAMSUNG CLOUD, que en los TÉRMINOS Y CONDICIONES[662] predispone que *"el presente Acuerdo y su relación con Samsung en virtud del presente Acuerdo se regirán e interpretarán de conformidad con las leyes de la jurisdicción en las que Usted reside, sin tomar en cuenta su conflicto con disposiciones legales y con sujeción a la jurisdicción no exclusiva de los tribunales de dicha jurisdicción, para resolver cualquier asunto legal que surja en relación con el Acuerdo"*. En el supuesto de ARSYS.ES[663], como ya hemos indicado, se establece que será la legislación española la aplicable en la interpretación y resolución de conflictos, así como en la regulación no contenida en el acuerdo. Sin embargo, no podemos olvidar que la compañía tiene domicilio social en España.

Entrando a analizar la validez material sobre la elección de la ley aplicable[664], los preceptos 67.1 y .2 del TRLCU delimitan y condicionan la posibilidad de elección de la ley aplicable cuando se contrata con consumidores. En primer lugar, prescribe que será el Reglamento Roma I quien determinará la ley aplicable, añadiendo, en el .2, que *"las normas de protección frente a las cláusulas abusivas contenidas en los artículos 82 a 91,*

---

661 CONDICIONES DEL SERVICIO DE GOOGLE, versión 25.10.2017. Accesible en: https://www.google.com/intl/es-419/policies/terms/. Último acceso: 08.08.2018.

662 TÉRMINOS Y CONDICIONES de SAMSUNG CLOUD, versión 08.08.2018. Accesible en: https://account.samsung.com/membership/terms. Último acceso: 08.08.2018.

663 CONDICIONES GENERALES DE SERVICIO de ARSYS a través del siguiente enlace: https://www.arsys.es/legal?dhtml=condiciones-generales-contratacion. Condiciones a fecha de 08.08.2018 (Ref.: CGS_23052018). Último acceso: 08.08.2018.

664 La validez formal la determina el Reglamento (CE) nº 593/2008 del Parlamento europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales, analizado en el subapartado *ii. Ámbito de aplicación*.

ambos inclusive, serán aplicables a los consumidores y usuarios, cualquiera que sea la ley elegida por las partes para regir el contrato, cuando este mantenga una estrecha relación con el territorio de un Estado miembro del Espacio Económico Europeo"[665][666]. Para las condiciones generales de contratación se recoge similar clausulado en el artículo 3.2 de la LCGC[667]. Por lo tanto, bien sea por la disposición imperativa establecida en el Reglamento Roma I, artículo 6.2, o porque el contrato mantenga una estrecha vinculación con algún Estado del Espacio Económico Europeo, será de aplicación la protección frente a las cláusulas abusivas.

Siendo de aplicación el TRLCU, el artículo 82.4.f) determina como abusivas las cláusulas que contravengan las reglas del derecho aplicable, consideración que debe completarse con el artículo 90.3, siendo abusivas las cláusulas que establezcan como ley aplicable aquella distinta *"respecto al lugar donde el consumidor y usuario emita su declaración negocial o donde el empresario desarrolle la actividad dirigida a la promoción de contratos de igual o similar naturaleza"*. Nótese que la declaración negocial puede realizarse en un estado, por manera accidental o incidental, donde no hay una vinculación efectiva. La clasificación como abusiva de la cláusula de elección de ley aplicable por el TRLCU difiere, respecto a los requisitos necesarios, como hemos

[665] El propio texto normativo define qué se entiende por vínculo estrecho: *"cuando el empresario ejerciere sus actividades en uno o varios Estados miembros del Espacio Económico Europeo, o por cualquier medio de publicidad o comunicación dirigiere tales actividades a uno o varios Estados miembros y el contrato estuviere comprendido en el marco de esas actividades"*. Es decir, el proveedor de servicios de *cloud* debe crear un vínculo con el país a través del ejercicio de acciones comerciales dirigidas al territorio y el contrato posterior debe surgir como consecuencia de dichas actividades.

[666] Una aplicación taxativa del artículo, como señala ÁLVAREZ DE SOTOMAYOR, llevaría a aplicar la legislación española, independientemente de la legislación elegida por las partes, siempre que el contrato mantuviera un vínculo de estrecha relación con cualquier Estado del Espacio Económico Europeo. ÁLVAREZ DE SOTOMAYOR, Silvia Feliu: "Nulidad de las cláusulas de jurisdicción y ley aplicable a la luz de la Ley 3/2014 por la que se modifica el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios", *Revista electrónica de estudios internacionales (REEI)*, 2015, nº 29, p. 19. Accesible en: http://www.reei.org/index.php/revista/num29/archivos/Estudio_FELIU_Silvia.pdf. Último acceso: 08.08.2018.

[667] *"La presente Ley se aplicará a las cláusulas de condiciones generales que formen parte de contratos sujetos a la legislación española.*
También se aplicará a los contratos sometidos a legislación extranjera cuando el adherente haya emitido su declaración negocial en territorio español y tenga en este su residencia habitual, sin perjuicio de lo establecido en los tratados o convenios internacionales. Cuando el adherente sea un consumidor se aplicará lo dispuesto en el apartado 3 del artículo 10 bis de la Ley General para la Defensa de Consumidores y Usuarios".

analizado *ad supra* y como reseña ÁLVAREZ DE SOTOMAYOR[668], con la consecuencia jurídica establecida en la norma de conflicto, es decir, la aplicación de la ley de la residencia habitual del consumidor, en defecto de elección.

En conclusión, el artículo 6.2 del Reglamento Roma I exige que la elección de la ley aplicable debe respetar, en todo caso, las normas estatales de carácter imperativo donde el consumidor tenga la residencia habitual, y el propio TRLCU, en el artículo 90.3, solo permite que los contratos del *cloud* con consumidores se rijan por la legislación del lugar donde se emite la declaración negocial por el consumidor o por la ley del Estado donde el empresario o profesional desarrolle la actividad dirigida a la celebración del contrato. Obliga, por tanto, a atender a la disposición contenida en el TRLCU dejando inoperativa la norma de conflicto establecida en el Reglamento Roma I.

e. Responsabilidad

La exclusión de la responsabilidad por parte del prestador de la nube es una de las cláusulas más controvertidas cuando la contraparte es un consumidor, aunque, como vimos en las relaciones B2B, no de manera exclusiva respecto a los contratantes. La indisponibilidad del servicio, la continuidad de la nube o, en general, cualquier prestación recogida en las condiciones generales, o en el ANS, que garantizan la correcta ejecución y calidad del servicio de computación en la nube determinan la responsabilidad del proveedor.

De forma genérica el artículo 86.1 del TRLCU prohíbe cualquier exclusión o limitación de los derechos legales que corresponden a los consumidores y usuarios por el incumplimiento, total, parcial o defectuoso, del proveedor de los servicios en la nube. Como señala CARBALLO FIDALGO[669], *"la norma acoge diversas manifestaciones de abuso en torno a los efectos de la inejecución del contrato"*, jurisprudenciales o legales,

---

[668] ÁLVAREZ DE SOTOMAYOR, Silvia Feliu: "Nulidad de las cláusulas de jurisdicción y ley aplicable a la luz de la Ley 3/2014 por la que se modifica el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios", *Revista electrónica de estudios internacionales (REEI)*, 2015, nº 29, p. 23. Accesible en: http://www.reei.org/index.php/revista/num29/archivos/Estudio_FELIU_Silvia.pdf. 08.08.2018.

[669] CARBALLO FIDALGO, Marta: "Las cláusulas en todo caso prohibidas (I)", *La protección del consumidor frente a las cláusulas no negociadas individualmente"*, 2013, Bosch, p. 152.

frente a un incumplimiento por parte del empresario o profesional, y por ende a la responsabilidad del proveedor.

Las cláusulas excluyentes de la responsabilidad, pérdida de acción, o de limitación de la responsabilidad, reducción de la pretensión del consumidor, se contemplan de manera expresa, como abusivas, en el artículo 86.2 del TRLCU[670]. De esta forma, sin exclusión, la normativa contempla como abusiva toda limitación de responsabilidad del empresario por incumplimiento contractual por daños. La extensión de la protección garantiza el correcto resarcimiento al consumidor, a través de la indemnización, de cualquier daño producido en el seno de la relación contractual. Es extensible para aquellas cláusulas que establecen un límite irrisorio como indemnización por un incumplimiento por la actitud empresarial.

Sin embargo, no establece el precepto la actitud del empresario o profesional en el desarrollo de la prestación del servicio en la nube. El artículo 1.102 del CC determina la exigibilidad, en todas las obligaciones, de la responsabilidad del empresario por una actitud dolosa, considerando nula la acción que establezca su renuncia. Si bien, el artículo 1.104 del CC habilita a las partes a determinar la extensión de la responsabilidad del proveedor del *cloud* atendiendo a la naturaleza, los sujetos intervinientes, el tiempo y el lugar, y recogiendo, ante la ausencia de regulación contractual, que se exigirá la del "buen padre de familia". Si entre empresarios una regulación de la limitación o exoneración de la responsabilidad del prestador del servicio puede ser perfectamente viable, con el límite de la actuación dolosa, cuando el contratante es un consumidor debe reportarse como cláusula abusiva, a tenor del artículo 86.1 del TRLCU. De otra forma, decaería la finalidad tuitiva de las normas de consumo, trasladando al cliente (consumidor) las consecuencias de un comportamiento no diligente del empresario.

Los proveedores de la nube, sobre todo aquellos que utilizan centros de datos fuera del EEE, intentan negar cualquier tipo de responsabilidad por daños directos, principalmente por la imposibilidad de acceder a los datos. En el EEE suele reconducirse la limitación a situaciones fuera del cuidado razonable y diligente, siempre respetando las técnicas y requisitos del sector, por ejemplo, a supuestos de fuerza mayor. Ante daños

[670] *"La exclusión o limitación de la responsabilidad del empresario en el cumplimiento del contrato, por los daños o por la muerte o por las lesiones causadas al consumidor y usuario por una acción u omisión de aquél"*.

indirectos, el estudio de la viabilidad jurídica de las cláusulas que excluyen o limitan la responsabilidad del prestador de servicios de *cloud* se dificulta. Determinar la responsabilidad del proveedor por pérdidas que no son previsibles en la formación del contrato, a lo que hay que añadir las dificultades y los riesgos del negocio del *cloud computing*, fundamenta que el empresario o profesional limite o excluya las consecuencias de estas pérdidas resultantes del cliente.

Esencial, para el *cloud*, es la regla establecida en el artículo 86.3 del TRLCU. La subcontratación de parte del servicio de la nube es práctica habitual del desarrollo de esta herramienta informática, limitando a recibir una compensación (motivo adicional para considerar abusiva una cláusula, conforme al artículo 82.4). Por lo tanto, determinar de manera expresa que el empresario o profesional principal, parte del contrato, no se libera de la responsabilidad contraída por la cesión a un tercero, sin consentimiento del consumidor, cayendo en abusiva la cláusula que así lo estableciera, facilita al cliente la reivindicación de la protección de sus datos.

La limitación de la cantidad económica a satisfacer por el proveedor, ante un daño del que es responsable, así como el supuesto de compensación de deudas no es más que la manifestación más visual de las cláusulas abusivas que estamos tratando. Sin embargo, ese límite no solo se manifiesta en términos económicos, a veces, el proveedor imposibilita al consumidor la posibilidad de plantear una acción, acotando un espacio temporal desde el daño excesivamente corto[671].

Sirvan algunos ejemplos para visualizar de forma práctica las cláusulas de exención.

SAMSUNG CLOUD en los TÉRMINOS DE SERVICIO ADICIONALES[672] limita su responsabilidad en el servicio, imponiendo cargas desproporcionadas al consumidor y trasladando sus obligaciones, al establecer que *"usted es responsable de realizar copias de seguridad de sus Contenidos en sus propios dispositivos de almacenamiento o soportes, puesto que Samsung no garantiza que usted pueda recuperar siempre los*

[671] En las cláusulas B2B ya estudiamos la imperatividad del plazo establecido para ejercer la acción por parte del cliente.

[672] TÉRMINOS DE SERVICIOS ADICIONALES DE SAMSUNG CLOUD, versión vigente a 08.08.2018. Accesible en: https://account.samsung.com/membership/etc/specialTC.do?fileName=personaldatamgmt.html. Último acceso: 08.08.2018.

Contenidos o las copias de seguridad de estos que almacene en los servicios SAMSUNG CLOUD". GOOGLE, dentro de las exenciones de responsabilidad, directamente indica que *"ni GOOGLE ni sus proveedores o distribuidores realizan promesa alguna específica sobre los servicios"*.

BOX[673] limita cualquier tipo de responsabilidad indirecta con la siguiente cláusula: *"bajo ninguna circunstancia BOX, sus subsidiarias, revendedores, funcionarios, empleados, agentes, proveedores o cedentes de licencias serán responsables por: cualquier daño indirecto, incidental, especial, de cubrimiento o consecuente (incluidos, entre otros, daños por ganancias perdidas, rendimiento, buena voluntad, uso o contenido) como sea que haya tenido lugar, bajo cualquier teoría de responsabilidad, incluidos, entre otros, contratos, agravios, garantías, negligencia o de cualquier otra forma, incluso si se ha aconsejado a box sobre la posibilidad de dichos daños"*. MICROSOFT[674] se manifiesta en similares términos[675], si bien, incluye un término importante, será responsable de los daños o perjuicios indirectos cuando *"hayan cometido, como mínimo, alguna negligencia grave o dolo"*. DROPBOX[676], bajo la premisa de que la limitación de responsabilidad se aplicará en los países en los que fuere posible, determina que no será responsable de *"(i) daños indirectos, especiales, fortuitos, punitivos, ejemplares o consecuentes; o (ii) pérdida de la utilización, datos, negocios o beneficios, independientemente de la condición jurídica"*.

La compañía española HOSTALIA[677] no excluye su responsabilidad en los supuestos de subcontratación al incluir en sus TÉRMINOS Y CONDICIONES DEL CONTRATO, en el apartado subcontratación, que *"será siempre responsable solidariamente del*

---

673 TÉRMINOS DE SERVICIO DE BOX, vigente desde 01.08.2017. Accesible en: https://www.box.com/es-419/legal/termsofservice. Último acceso: 08.08.2018.

674 Apartado de MICROSOFT SERVICES AGREEMENT, versión 01.03.2018. Accesible en: https://www.microsoft.com/en-us/servicesagreement/. Último acceso: 08.08.2018.

675 *"Ni Microsoft, ni sus agentes subsidiarios ni sus representantes legales serán responsables de ningún daño o perjuicio indirecto, lo que incluye la pérdida económica como, por ejemplo, la pérdida de beneficios…"*.

676 CONDICIONES DE SERVICIO DE DROPBOX, versión 14.04.2018. Accesible en: https://www.dropbox.com/privacy#terms. Último acceso: 08.08.2018.

677 TÉRMINOS Y CONDICIONES DEL CONTRATO de HOSTALIA, versión a 08.08.2018. Accesible en: https://www.hostalia.com/contratar/contrato/. Último acceso: 08.08.2018.

cumplimiento del Contrato y de todas las obligaciones derivadas del mismo frente al Cliente". Para el servicio FLEXIANT CLOUD ORCHESTRATOR[678], el proveedor excluye su responsabilidad en el caso de pérdidas y uso de datos (*"loss of data or use of data"*), y lo que es más preocupante, excluye su responsabilidad en caso de pérdida o daño indirecto, incluso si tuvieran o hubieran sido advertidos de tal posibilidad (*"...even if we knew, have reason to know or have been advised of the possibility of such loss or damage..."*)

HOSTALIA limita la responsabilidad a la *"suma de todas las cantidades abonadas por el Cliente durante los últimos seis (6) meses precedentes a la producción del evento causante del daño"*. Curioso es el límite económico que impone BOX, como responsabilidad total, determinándose al *"al mayor de: a) una vez y media (1,5) la tarifa mensual o anual más reciente que usted haya pagado por ese servicio; o b) cien dólares (100 USD)"*, siempre y cuando la pérdida o daño no sea menor al criterio establecido. Irrisoria la cantidad económica establecida, 100 USD.

f. Uso aceptable

Los proveedores en la política de usos aceptables suelen recoger un conjunto de actividades o comportamientos para el correcto desarrollo de la nube o, incluso, como medida preventiva en la comisión de infracciones[679]. Algunas de las prohibiciones más comunes hacen referencia al uso de la herramienta para SPAM, el alojamiento de contenido que incite al odio o la discriminación, la disposición e intercambio de archivos amparados en los derechos de propiedad intelectual e industrial y el intercambio de contenido pedófilo.

Dentro de este elenco de medidas, las cláusulas recogidas en la política de usos aceptables se considerarán irrazonable o injustas cuando dependa exclusivamente del proveedor de servicios en la nube, de su cuidado y pericia, el correcto funcionamiento del servicio. En caso contrario, habrá que determinar el grado de responsabilidad de las partes. No podemos olvidar que es obligación del cliente de la nube el cumplimiento de la AUP.

---

[678] FLEXIANT CLOUD ORCHESTRATOR END USER LICENCE AGREEMENT, version FEUL-2013022501. Accesible en: https://www.flexiant.com/support/eula/. Último acceso: 08.08.2018.

[679] Véase el Capítulo V.a.b.ii)

Ante una infracción del consumidor de las políticas de usos aceptables, al parecer del prestador del servicio, la medida a tomar suele ser la retirada o suspensión del servicio, sin previo aviso al consumidor o usuario, por considerar que este incumple las reglas de uso aceptable o las condiciones de uso que el proveedor establece de manera unilateral, eximiéndose de cualquier perjuicio, económico o no, que pueda ocasionar en el cliente. Esta actuación claramente contraviene los dictados establecidos en el TRLCU, debiendo ser considerada la medida abusiva, al ser el profesional del servicio el que decide cuándo se ha incumplido por el consumidor esas reglas de uso aceptable, de manera unilateral. Es decir, no existe posibilidad de contradicción o argumentación. Incluso, el proveedor de *cloud* puede "fallar" la sanción ante tal conducta. Si el proveedor, además, recoge en las cláusulas no negociadas la posibilidad de rescindir el contrato ante la actuación del consumidor, de manera unilateral y discrecional, sería considerada abusiva por falta de reciprocidad, a tenor del artículo 87.3 del TRLCU[680]. Esta argumentación se refuerza, aun más, cuando el proveedor predispone que no devolverá las cantidades económicas al cliente por los servicios no devengados[681].

La facultad de retirar los datos o aplicaciones, por parte del proveedor, cuando considere, a su juicio, que el consumidor ha incumplido con las condiciones establecidas en el contrato y/o en alguno de sus anexos, recurrente en los contratos en la nube, se estudiará en el subapartado *"localización y tratamiento de datos"*.

Para la nube OFFICE 365 de MICROSOFT, el CODE OF CONDUCT[682] posibilita al proveedor a dejar de ofrecer los servicios, e incluso cerrar la cuenta o bloquear los servicios, si no se cumplen los términos sobre el uso del servicio, incluso pudiendo revisar por completo el contenido establecido en la nube[683]. Por lo tanto, una política de usos que

---

[680] Cláusula abusiva por falta de reciprocidad, artículo 87.3 del TRLCU: *"La autorización al empresario para resolver el contrato discrecionalmente, si al consumidor y usuario no se le reconoce la misma facultad"*.

[681] Conforme al artículo 87.4 del TRLCU, la cláusula es abusiva si establece *"la posibilidad de que el empresario se quede con las cantidades abonadas en concepto de prestaciones aún no efectuadas cuando sea él mismo quien resuelva el contrato"*.

[682] Apartado de MICROSOFT SERVICES AGREEMENT, versión 01.03.2018. Accesible en: https://www.microsoft.com/en-us/servicesagreement/. Último acceso: 08.08.2018.

[683] Cláusula original: *"Enforcement. If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account or Skype account. We may also block delivery of a communication (like email or instant message) to or from the Services in an effort to enforce these Terms or we may remove or refuse to publish Your Content for any reason. When investigating alleged violations of these Terms,*

podría ser perfectamente válida, por cuanto solo hace referencia a comportamientos claramente ilícitos de usuarios, produce consecuencias que, al amparo del TRLCU, dificultan su aplicación, al atribuir al proveedor la facultad, sin delimitar ningún tipo de comunicación con el cliente, de suspender, bloquear o eliminar la información o los datos que contengan.

WNPOWER, que ofrece servicio de *cloud* para empresas y consumidores de habla hispana, por lo tanto se dirige expresamente al mercado español, establece en su POLÍTICAS DE USO ACEPTABLE[684] que *"en ningún caso de suspensión o rescisión previsto se generará ningún tipo de indemnización a cargo de WNPOWER, la que podrá reclamarle al cliente o usuario los daños y perjuicios, directos e indirectos, ocasionados por la realización de la conducta prohibida en la presente Política"*, produciéndose un claro desequilibrio entre las facultades del proveedor y cliente.

g. Localización y tratamiento de datos

Los proveedores del servicio en la nube pueden indicar en su oferta dónde se localizan sus servicios o las zonas regionales donde operan los servidores, es decir, dónde se guardará la información y los datos del cliente. ARSYS y ACENS, entre otros, indican en la oferta dónde se ubican sus servidores: ARSYS posibilita a elegir entre EE.UU. o España, y ACENS directamente establece sus centros de datos en Madrid . Será, por tanto, necesario atender al correcto cumplimiento de la oferta por parte del proveedor, si no decaería en una práctica comercial desleal, y la correcta aplicación de la normativa de protección de datos. En similares términos nos pronunciamos sobre el monitoreo de la información y los datos por parte de los proveedores.

Importante es conocer qué sucederá con los datos que el consumidor, en la prestación del servicio, emplea en la nube terminado o rescindido el contrato. El borrado inmediato o el establecimiento de un período de recuperación de datos[685], antes de la eliminación definitiva, o, incluso, el establecimiento de la facultad de decidir por el proveedor del

---

Microsoft reserves the right to review Your Content in order to resolve the issue. However, we cannot monitor the entire Services and make no attempt to do so".

[684] POLÍTICAS DE USO ACEPTABLE, versión a 08.08.2018. Accesible en: https://www.wnpower.com/empresa/politicas-uso-aceptable-pua. Último acceso: 08.08.2018.

[685] En el capítulo III.b, estudios del Grupo de Trabajo del artículo 29, y en el capítulo IV determinamos el régimen del cliente, ahora consumidor, en el tratamiento de datos personales, así como las obligaciones y las responsabilidades que tal condición le imponen.

borrado inmediato o el período de gracia, son las alternativas que plantean los proveedores del *cloud*. La primera propuesta aparece, por ejemplo, en los contratos con MICROSOFT (*"eliminaremos los Datos o Su Contenido asociados a la cuenta de Microsoft o la cuenta de Skype o los desvincularemos de la cuenta de Microsoft o Skype (a menos que la legislación aplicable nos obligue a conservarlos)*); la segunda opción, en el contrato con DROPBOX ("*Finalización de los servicios: … Te avisaremos con una antelación razonable a través de la dirección de correo electrónico asociada a tu cuenta, a fin de poner remedio a la actividad que nos ha llevado a contactar contigo, y te daremos la oportunidad de exportar tu Contenido fuera de nuestros Servicios"*)[686] o CLOUD de A3 SOFTWARE[687] (*"una vez finalizado el contrato A3 SOFTWARE pondrá a disposición del Cliente un archivo de datos del mismo durante los 30 días siguientes a la terminación, solo si el Cliente así lo ha manifestado en el momento en que tenga lugar la finalización*) ;y del tercer tipo de reglamentación, la establecida con HUAWEI CLOUD (*"after your account is terminated, Huawei may immediately and permanently delete any and all of the data, files and stored contents under your account"*).

Sin entrar a valorar lo dispuesto en la normativa de protección de datos personales sobre la preservación de datos y el derecho a la portabilidad, reconocido expresamente en el artículo 20 del RGPD, nada dispone la Directiva 93/13/CEE o el TRLCU sobre la facultad del consumidor de recuperar sus datos finalizado o rescindido el contrato o, en último caso, de la eliminación inmediata de datos. Sí se establece, en el artículo 60.2.i) del TRLCU, como información previa al contrato de la nube, la obligación al proveedor de facilitar *"la funcionalidad de los contenidos digitales, incluidas las medidas técnicas de protección aplicables, como son, entre otras, la protección a través de la gestión de los derechos digitales o la codificación regional"* y, artículo 60.2.j) del TRLCU, de *"toda interoperabilidad relevante del contenido digital"*.

[686] Hay que indicar que supone una modificación respecto a las cláusulas establecidas en el contrato con profesionales o empresarios, que recoge, expresamente, que (efectos de la finalización) *"Dropbox podría eliminar los Datos del Cliente almacenados de la cuenta del Cliente"*. Si bien, en el supuesto de contratación con consumidores no establece el plazo de recuperación de los datos, estableciendo una serie de supuestos donde no dispondrá el cliente de esa facultad.

[687] CONDICIONES PARTICULARES DEL CONTRATO DE SERVICIOS CLOUD de A3 SOFTWARE, versión vigente 08.08.2018. Accesible en: https://media.a3software.com/cloud/Condiciones%20particulares%20contrato%20servicios%20cloud.pdf. Último acceso: 08.08.2018.

h. Garantías y devolución del crédito por servicios no consumidos

Se ha tratado cómo afecta la normativa de protección de los consumidores en las cláusulas sobre la responsabilidad de los proveedores en la ejecución del servicio. Un estudio completo requiere el análisis de las garantías y la posibilidad de la devolución de los créditos por los servicios no consumidos, por terminación anticipada o rescisión del contrato.

MICROSOFT[688] establece en su sistema de garantías que es *"obligación de Microsoft prestar los Servicios con diligencia y cuidado razonables"*, sin que ninguna prescripción esté destinada a *"limitar o excluir la responsabilidad por incumplimiento de esto por parte de Microsoft"*. Sin embargo, y salvo defectos ocultos de mala fe o que impidan el uso del servicio, no garantizan *"la exactitud ni puntualidad de la información disponible"*, haciendo recaer en el cliente (*"usted reconoce y acepta"*) que los equipos informáticos no están libres de defectos o períodos de inactividad, no proporcionando ninguna garantía adicional, y excluyendo *"todas las garantías obligatorias implícitas"*.

No es ninguna excepción el contenido establecido por MICROSOFT. GOOGLE[689] va más allá. Manifiesta que no *"realizan promesa alguna específica sobre los servicios"*, no asumiendo *"ningún compromiso respecto al contenido de los servicios, la función específica de los servicios…"*, añadiendo que proporcionan los servicios *"tal como están"*. Incorpora, además, una "cláusula salvatoria", con las consecuencias jurídicas anteriormente señaladas, indicando que *"…en la medida permitida por ley, excluimos todas las garantías"*. Sin embargo, uno de los supuestos más relevantes de los estudiados es FACEBOOK[690]. El proveedor, siempre que actúe con "pericia" predispone que *"no*

[688] Apartado de MICROSOFT SERVICES AGREEMENT, versión 01.03.2018. Accesible en: https://www.microsoft.com/en-us/servicesagreement/. Último acceso: 08.08.2018.

[689] CONDICIONES DEL SERVICIO DE GOOGLE, versión 25.10.2017. Accesible en: https://www.google.com/intl/es-419/policies/terms/. Último acceso: 08.08.2018.

[690] CONDICIONES DEL SERVICIO de FACEBOOK, fecha de revisión 19.04.2018. Accesible en: https://www.facebook.com/legal/terms/update. Último acceso: 08.08.2018.

asumimos responsabilidad alguna por: pérdidas no provocadas por la infracción por nuestra parte de estas Condiciones o como consecuencia de nuestras acciones"[691].

Por lo tanto, de una forma u otra los prestadores del servicio de la nube niegan, en algunos supuestos de manera total, cualquier tipo de garantía, implícita e, incluso, explícita por algunos proveedores, que aseguren el adecuado funcionamiento del servicio conforme al desarrollo formulado. El artículo 86.1 del TRLCU prescribe que serán abusivas aquellas cláusulas que limiten los derechos básicos del consumidor, en particular, aquellas que excluyan o limiten de forma inadecuada los derechos legales del consumidor y usuario por incumplimiento, total o parcial, o cumplimiento defectuoso.

Supuesto particular de cláusula abusiva es la privación o restricción al consumidor de las facultades de compensación de créditos, retención o consignación, artículo 86.4 del TRLCU. Los proveedores de la nube que limiten la posibilidad de compensación o devolución de las cantidades cobradas y no consumidas por el cliente, cuando depende del comportamiento o actuación del prestador del servicio, actuarán de forma negligente. Para el servicio de ICLOUD[692], APPLE se compromete a la devolución del pago realizado por los consumidores *"por adelantado por el período de pago actual en ese momento"* ante cambios sustanciales en la nube o en sus condiciones de uso. Sin embargo, sí contempla la totalidad del reembolso de la cantidad económica satisfecha por el cliente cuando, y dentro de un período de 14 días desde la notificación por correo electrónico de la activación del servicio, el cliente manifieste su deseo de cancelar el servicio, sin ningún coste por el reembolso. No discute ni regula otras posibilidades de terminación o rescisión del contrato. Este "período de reflexión" también está presente en los servicios de MICROSOFT[693], coincidiendo en el número de días, pero desde la adquisición del servicio, añadiendo que si se ha hecho uso de forma parcial, se recibirá la devolución de forma prorrateada.

---

[691] Esta cláusula ya supone un avance en el equilibrio entre partes. En la DECLARACIÓN DE DERECHOS Y RESPONSABILIDADES de FACEBOOK de 30.01.2015 se establecía, expresamente, *"*(los servicios se proporcionan) *tal cual, sin garantía alguna expresa o implícita"*.

[692] TÉRMINOS Y CONDICIONES DE ICLOUD de APPLE, versión de 19.09.2017. Accesible en: https://www.apple.com/legal/internet-services/icloud/es/terms.html. Último acceso: 08.08.2018.

[693] Apartado de MICROSOFT SERVICES AGREEMENT, versión 01.03.2018. Accesible en: https://www.microsoft.com/en-us/servicesagreement/. Último acceso: 08.08.2018.

El ámbito de aplicación planteado excluye los supuestos de cancelación o resolución del contrato por una actuación negligente del consumidor, que deberá analizarse conforme a lo dictado en el artículo 85.6 del TRLCU y determinar, por tanto, si las arras penales superan los criterios de proporcionalidad.

i. Acuerdos de Nivel de Servicios, cambios y renovación.

Siguiendo la clasificación de TUR FAÚNDEZ[694], los supuestos más comunes en los que el empresario o profesional recoge en el clausulado del contrato las posibilidades de modificar unilateralmente algunas de las condiciones inicialmente presentadas son:

- La alteración de las condiciones del servicio del *cloud*, a fin de adaptar la nube al estado de la técnica u otras circunstancias que lo justifiquen.
- La posibilidad de proceder a la cancelación del servicio de manera definitiva, normalmente avisando al cliente con cierta antelación; o la suspensión temporalmente el servicio para solventar o mejorar cuestiones técnicas, comunicándolo previamente al consumidor.
- El cambio de la política de costes, exigiendo una contraprestación económica por servicios que anteriormente realizaba de manera gratuita, notificando al cliente dicha medida con un plazo de antelación razonable, en el cual si el cliente no se manifiesta se entiende que acepta las condiciones.
- Modificación, por el proveedor, de los precios establecidos, notificando a los clientes con un breve plazo de tiempo. En este supuesto, normalmente, si el cliente muestra su disconformidad puede unilateralmente rescindir el contrato.
- Imposición de la facultad para suspender el servicio en caso de impago de la contraprestación económica, o cuando exista un alto riesgo de no pagarlas.

En los supuestos contemplados se ha considerado que el prestador del servicio de la nube informa de manera previa y faculta al cliente, en un período de tiempo razonable, a adoptar las medidas que considere oportunas tras la modificación de las variaciones del contrato. El estudio realizado en el subapartado *"b. Variación de los términos del*

[694] TUR FAÚNDEZ, María Nélida: "La responsabilidad contractual de los intermediarios electrónicos", *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, Comares, 2005, p. 149-151.

contrato" es perfectamente replicable, realizando el análisis por separado solo a efectos de una mejor exposición.

Es esencial determinar el carácter de la reserva para suspender el servicio de forma unilateral, no tratada anteriormente, aun en los supuestos de notificación y aviso al cliente en un período razonable. Sería oportuno distinguir entre el carácter económico del servicio y la duración. Si el consumidor ha satisfecho una cantidad económica por adelantado y por un tiempo determinado, el proveedor deberá restituir la cantidad económica no satisfecha. Si la nube es "gratuita" y sin establecerse un período de finalización, será considerada válida siempre que cumpla los criterios de transparencia y equilibrio. Todo ello sin perjuicio de la posibilidad de reclamar indemnización por daños y perjuicios causados ante el incumplimiento de las obligaciones contractuales, siempre que incurriere el proveedor de servicios en dolo, negligencia o morosidad, artículo 1.101 del CC. El diferente régimen de nulidad en función de la duración del contrato también es defendido por CARBALLO FIDALGO[695] y por nuestro Alto Tribunal[696]. En resumen, el carácter abusivo ante contratos de duración determinada depende de la existencia de idéntica facultad para el consumidor, y el carácter abusivo de la nube con duración indefinida se condiciona a la notificación previa al consumidor y al plazo razonable de comunicación.

La cláusula que establezca la posibilidad de rescindir unilateralmente el contrato por el proveedor de la nube decaería en abusiva por falta de reciprocidad, según el artículo 87.3 del TRLCU[697]. Desde nuestro punto de vista, además, debe ser considerada abusiva a tenor del artículo 85.3 y .4 del TRLCU[698], al dejar a juicio del profesional de la nube la

---

[695] CARBALLO FIDALGO, Marta: "Las cláusulas en todo caso prohibidas (I)", *La protección del consumidor frente a las cláusulas no negociadas individualmente"*, 2013, Bosch, p. 136.

[696] En otras, la Sentencia del Tribunal Supremo de 25 de mayo de 2009, núm. 3491/2009. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=4616972&links=abusiva&optimize=20090625&publicinterface=true. Último acceso: 08.08.2018.

[697] *"La autorización al empresario para resolver el contrato discrecionalmente, si al consumidor y usuario no se le reconoce la misma facultad"*.

[698] *"3. Las cláusulas que reserven a favor del empresario facultades de interpretación o modificación unilateral del contrato, salvo, en este último caso, que concurran motivos válidos especificados en el contrato.*

...

4. Las cláusulas que autoricen al empresario a resolver anticipadamente un contrato de duración determinada, si al consumidor y usuario no se le reconoce la misma facultad, o las que le faculten a resolver

correcta actuación del consumidor, y, por tanto, su incumplimiento, estableciendo las medidas sancionadoras que considere necesarias, entre ellas la no prestación del servicio acordado con el usuario de manera eficiente.

MICROSOFT[699] predispone que si puntualmente no recibe el pago del servicio se procederá a la suspensión o cancelación del servicio, a su elección, tras su notificación. No establece, sin embargo, el período de suspensión, ni el plazo del que dispone el consumidor para realizar el pago desde la comunicación del proveedor. DROPBOX[700], para sus cuentas de pago, establece que *"podríamos cambiar las tarifas vigentes, pero te avisaremos por adelantado de dichos cambios mediante un mensaje a la dirección de correo asociada a tu cuenta"*, nada dice de las facultades del consumidor ni de plazos de ejercicio. Cláusula similar regula el supuesto de suspensión de los servicios[701], si bien, reconociendo el reintegro del importe satisfecho.

j. Extinción del contrato.

En el estudio de la prestación del servicio de la nube entre empresas hemos debatido sobre la extinción del contrato, sus causas y efectos. Si el contratante del servicio es un consumidor, algunas de las cláusulas indicadas pueden considerarse abusivas.

Debe partirse del análisis de la prescripción establecida en el artículo 62.4 del TRLCU. Ante la contratación de servicios o suministros, el contrato debe establecer "expresamente" el procedimiento para poner fin a la relación por parte del usuario cuando no tenga duración determinada. En los contratos analizados se recogía, de forma meridianamente clara, el proceder para el desistimiento y la resolución por incumplimiento de alguna de las partes.

---

los contratos de duración indefinida en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable".

[699] Apartado de MICROSOFT SERVICES AGREEMENT, versión 01.03.2018. Accesible en: https://www.microsoft.com/en-us/servicesagreement/. Último acceso: 08.08.2018.

[700] CONDICIONES DE SERVICIO DE DROPBOX, versión 17.04.2018. Accesible en: https://www.dropbox.com/privacy#terms. Último acceso: 08.08.2018.

[701] *"Podríamos decidir suspender los Servicios como respuesta a circunstancias imprevistas que escapen al control de Dropbox, o bien para cumplir algún requisito legal. De ser así, te avisaremos con la suficiente antelación para que puedas exportar tu Contenido y sacarlo de nuestros sistemas. Si suspendemos los Servicios de esta forma antes de que acabe un plazo fijo o mínimo por el que nos hayas pagado previamente, te reembolsaremos la parte proporcional del importe satisfecho".*

Sin embargo, sí se presentan dificultades cuando el consumidor opta por el desistimiento unilateral del servicio. Problemas como períodos de permanencia con una duración excesiva[702] o la cancelación del servicio por el proveedor sin previo aviso son cláusulas comunes en las condiciones generales de los grandes proveedores.

FACEBOOK[703] establece *"si determinamos que has infringido nuestras condiciones o políticas, especialmente nuestras Normas comunitarias, de manera notoria o grave, o en reiteradas ocasiones, es posible que suspendamos o inhabilitemos definitivamente tu cuenta. También es posible que suspendamos o inhabilitemos tu cuenta si la ley así lo exige. Cuando corresponda, te notificaremos…"*. Se deja, a elección del proveedor, la posibilidad de notificar la cancelación o suspensión del servicio, al no regularse los supuestos ante los que es obligatoria la notificación. GOOGLE, en sus CONDICIONES DE SERVICIO[704], establece que *"si interrumpimos un Servicio, en los casos en los que sea razonable, te informaremos con suficiente antelación y te permitiremos extraer la información del Servicio"*, pero nada indica acerca de la suspensión o cancelación de los servicios de forma unilateral.

El artículo 85.4 del TRLCU considera abusivas las cláusulas que posibilitan al empresario resolver el contrato sin la previa notificación, que debe tener una "antelación razonable".

[702] El artículo 62.3 del TRLCU prohíbe *"las cláusulas que establezcan plazos de duración excesiva o limitaciones que excluyan u obstaculicen el derecho del consumidor y usuario a poner fin al contrato"*. Dependerá del servicio para determinar si el plazo de permanencia es excesivo. Entre otros condicionantes, influirá, los costes asociados al desarrollo del servicio que tiene que afrontar el proveedor, por ejemplo, ante la compra de servidores exclusivos para el cliente. La Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales, COM/2015/0634 final, considera que el consumidor tiene derecho a resolver los contratos cuando el período de expiración del mismo exceda los 12 meses, artículo 16.

[703] CONDICIONES DEL SERVICIO de FACEBOOK, revisión de 19.04.2018. Accesible en: https://www.facebook.com/legal/terms/plain_text_terms. Último acceso: 08.08.2018.

[704] CONDICIONES DE SERVICIO de GOOGLE, versión de 25.10.2017 (vigente a 08.08.2018). Es aplicable, entre otros, a los servicios de GMAIL. Accesible en: https://policies.google.com/terms?hl=es. Último acceso: 08.08.2018.

c. La contratación del *cloud computing* en el sector público

a. *El empleo de los medios electrónicos en las Administraciones públicas. Mimbres para la utilización de la nube.*

La utilización del *cloud computing* como herramienta de gestión en las Administraciones públicas se viene debatiendo desde la aparición del recurso informático[705]. La decisión de implantar la nube y los niveles de uso de la herramienta puede estudiarse desde diferentes perspectivas. En primer lugar, en función de la actuación de las Administraciones como agentes en la contratación, pueden actuar como clientes o proveedores para empresas u otras Instituciones públicas. En otro orden, las Administraciones pueden incentivar a las empresas, con ayudas financieras y actividades de consolidación, a la adopción de la tecnología[706]. Y, por último, es importante determinar el uso de la nube dentro de la organización por el personal vinculado a una relación laboral con las Administraciones públicas. Es decir, determinará la incidencia de la herramienta informática si el *cloud* solo se destina a un uso individual, no colaborativo, en el puesto de trabajo, como herramienta para conseguir ser más eficaz en las tareas y rutinas que cada persona desarrolla en su día a día; si se emplea por un colectivo concreto, compartiendo, en grupo, un conjunto cerrado datos, trabajos e información; o, con una visión más expansiva y extensiva, el uso institucional de la nube se configura como política estratégica de la organización en los métodos de trabajos e interrelación. Sin olvidar, por otra, que la nube puede ser utilizada *ad intra* o *ad extra*, ya sea entre diferentes Instituciones del sector público y/o para las diferentes comunicaciones entre los administrados.

La adopción de este sistema tecnológico no está exenta de obstáculos, de índole política (por los recelos de las Instituciones en compartir datos con diferentes Administraciones u organismo/entes), y de carácter legal, derivados de la necesidad de proteger la seguridad del Estado, los derechos y libertades de las personas o la propia

[705] PALOMAR I BAGET, en 2014, afirmaba que se debe incidir en herramientas colaborativas en la nube que permitan al personal al servicio del sector público ser más eficientes con el uso de las TIC. PALOMAR I BAGET, Jesús: "Cómo empezar a utilizar herramientas en la nube en nuestra administración", *Redes sociales y herramientas en la nube para las administraciones públicas del siglo XXI*, 2014, p. 24-25. En: http://www.eudel.eus/es/archivos/libro/redes_socilaes_y_herramientas.pdf. Último acceso: 08.08.2018.

[706] MAQUERIRA MARÍN, Juan Manuel y BRUQUE CÁMARA, Sebastián: "Agentes impulsores de la adopción de cloud computing en las empresas. ¿Quién mueve la nube?", *Universia Business Review*, 2012, p. 56-77.

misión del ente público en cuestión[707]. Los primeros intentos de implantación de un sistema tecnológico de acceso amplio tenían como finalidad que los trabajadores del sector público pudieran desarrollar su prestación de servicios sin necesidad de encontrarse en un puesto de trabajo concreto. El teletrabajo en las Administraciones públicas ha sido un concepto recurrente en la última década. Con la implantación del *cloud computing*, la tecnología mejor posicionada al proporcionar servicios online accesibles desde cualquier terminal de cualquier usuario, se llevaría a cabo un importante ahorro en costes en los edificios públicos, teniendo en cuenta que las distintas Instituciones públicas cuentan, en sumatorio, con más de dos millones y medios de efectivos[708]. Sin embargo, no solo las mejoras en costes incentivan al sector público a buscar nuevas alternativas, siendo la eficiencia en la gestión interna, de forma global, el objetivo necesario para la adopción de nuevas herramientas TIC. El Observatorio de Administración Electrónica (OBSAE)[709] considera al *cloud computing* como modelo de referencia para la provisión de los servicios TIC dentro de las Administraciones públicas.

CAMPOS ACUÑA[710], que analiza la experiencia de la herramienta FACe, resalta que la primera ventaja que deriva de esta herramienta TIC colaborativa, impuesta a las Administraciones públicas españolas, es la homogeneidad en la definición de un modelo, todas las Administraciones públicas y el sector privado, con independencia del nivel territorial de la Administración pública con la que se relacione, deben emplear la herramienta, proporcionando, a efectos internos, interoperabilidad e implantación generalizada. Sirva de ejemplo que el Gobierno de España estima que, si pasamos de presentar una solicitud presencial (coste 80€) a presentar una solicitud electrónica (coste

[707] GARCÍA MEXÍA, Pablo: "Cloud computing: Sus implicaciones legales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2010, nº 23, p. 84-85.

[708] Fuente: Boletín Estadístico del Personal al Servicio de las Administraciones Públicas – Registro Central de Personas, enero 2017 (última publicación a 02.01.2018). Accesible en: http://www.sefp.minhafp.gob.es/dam/es/web/publicaciones/centro_de_publicaciones_de_la_sgt/Periodicas/parrafo/Boletin_Estadis_Personal/B_enero_2017_BIS.PDF.PDF. Último acceso: 08.08.2018.

[709] OBSERVATORIO DE ADMINISTRACIÓN ELECTRÓNICA (OBSAE): "Hacia una estrategia de Cloud Computing en las Administraciones Públicas", *Notas técnicas*, 2013, febrero, p. 1. Accesible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:99490b88-c2d4-4ca1-b16e-140fa7caf13c/2013-02_nota_tecnica_CLOUD.pdf. Último acceso: 08.08.2018.

[710] CAMPOS ACUÑA, María Concepción: "Implantación de la administración electrónica. 5 lecciones que aprender de la experiencia FACe", *La Administración Práctica,* 2017, Cizur Menor, núm. 5/2017, parte análisis doctrinal. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

5€) el ahorro que se obtiene es 75€[711]. El acceso a la información e innovación en la gestión, necesarios para la efectiva transparencia en las Administraciones públicas y para una participación activa, propiciando una mayor eficiencia, hace necesario la informatización de las Instituciones, agilizando, simplificando y eliminando tareas que se realizan de forma duplicada. Por lo tanto, el *cloud*, junto con una revisión estratégica de la gestión administrativa, se propugna como herramienta necesaria. La Agenda Digital para España[712], en los planes y actuaciones, establece una hoja de ruta, incumplida, para la implantación de las nuevas tecnologías y la E-administración[713].

Con estos condicionantes, se hace necesario el estudio de la contratación de la computación en la nube por las Administraciones públicas. Dejando a un lado los problemas de índole política que puede suponer la contratación del *cloud*, y centrándonos en la actuación de las Instituciones del sector público como demandantes de la prestación del servicio, será el encuadre con la normativa española lo que determinará su implantación efectiva.

Debemos tener presente en todo momento las especialidades derivadas de la normativa administrativa, sobre todo en el análisis del acceso a la información subida al entorno de la nube. El propio artículo 105.b) de la Constitución Española[714] faculta a los ciudadanos a acceder a la información que contienen los archivos y registros administrativos, señalando que mediante Ley se regulará dicho acceso, salvo que afecte a la seguridad y defensa del Estado, la averiguación de delitos y/o la intimidad de las personas. Los límites se encuentran, actualmente, en el artículo 13 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

[711] Cálculos obtenidos del "Método simplificado de medición de cargas administrativas", obtenido a través de la "Aplicación para la medición de las cargas administrativas" de la herramienta APLICA, diseñada por el Ministerio de Hacienda y Administraciones Públicas. Es accesible, bajo registro en la red SARA, en: https://administracionelectronica.gob.es/ctt/aplica. Último acceso: 02.01.2018.

[712] Accesible en: http://www.agendadigital.gob.es/planes-actuaciones/Paginas/planes-actuaciones.aspx. Último acceso: 08.08.2018.

[713] Para nuestro estudio, se recomienda leer el Plan de impulso de la economía digital y los contenidos digitales, junio 2013, y el Plan de Servicios Públicos Digitales, junio 2014. Accesibles, respectivamente: http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecacontenidos/Detalle%20del%20Plan/Plan-ADpE-3_Contenidos.pdf y http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaserviciospublicos/Detalle%20del%20Plan/Plan-ADpE-8_ServiciosP%C3%BAblicos.pdf. Últimos accesos: 08.08.2018.

[714] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229. Último acceso: 08.08.2018.

(LPACAP)[715] y el artículo 14 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[716] [717]. A pesar de las reformas y mejoras aportadas por la LPACAP, aún no se ha promulgado ninguna Ley específica que regule tal derecho de acceso de forma completa. Por lo tanto, cuando una Institución pública contrata los servicios de computación en la nube debe garantizar que los ciudadanos puedan ejercer el derecho de acceso a la información contenida en los archivos públicos, y, por otro lado, que la información restringida o limitada por la normativa se proteja con medidas de seguridad apropiadas. Como señalaba ACÍN FERRER[718], la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAE)[719], derogada por la LPACAP, no logró una aplicación generalizada de los medios electrónicos como forma normal de tramitación de los procedimientos administrativos por carecer, muchas de las Administraciones públicas, de los medios personales y técnicos para garantizar el mandato constitucional. Sin querer distraernos del objeto de estudio, deberán ser las Diputaciones provinciales o entidades equivalentes las encargadas de implementar la informatización en las entidades locales con menos de 20.000 habitantes[720]. Así lo ha declarado el Tribunal Constitucional en la Sentencia

---

[715] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565. Último acceso: 08.08.2018.

[716] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20131221&tn=2. Último acceso: 08.08.2018.

[717] En lo que respecta a la LPACAP señala *"e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones."* y *"h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas"*.

La Ley 19/2013, de 9 de diciembre, dedica el artículo a los límites al derecho de acceso cuando suponga un perjuicio para *"a) La seguridad nacional, b) La defensa, c) Las relaciones exteriores, d) La seguridad pública, e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva, g) Las funciones administrativas de vigilancia, inspección y control, h) Los intereses económicos y comerciales, i) La política económica y monetaria, j) El secreto profesional y la propiedad intelectual e industrial, k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión, l) La protección del medio ambiente"*.

[718] ACÍN FERRER, Ángela: "Procedimiento administrativo. Administración electrónica. Derecho de acceso a la información. La difícil aplicación de la Ley del Procedimiento Administrativo Común", *La Administración Práctica,* 2015, Cizur Menor, núm. 6/2015, parte comentario. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

[719] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352. Último acceso: 08.08.2018.

[720] La Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local, de racionalización y sostenibilidad de la Administración Local modificó el artículo 36 de la Ley 7/1985, de 2

número 111/2016, de 9 de junio de 2016[721], al establecer que *"lo que pretende el precepto es dar efectividad a la prestación de unos servicios que exigen la aplicación de tecnología informática (en el caso de la administración electrónica) o técnico-jurídica (en el supuesto de la contratación centralizada) que los municipios de pequeña o mediana población (hasta 20.000 habitantes), pueden no estar en condiciones de asumir"*.

El primer intento de transformación digital de las Administraciones públicas en España viene de la mano de la LAE, si bien, desde su promulgación se cuestionaba la idoneidad de los preceptos contenidos en la norma, centrando la discusión en si suponía nuevas formas y modalidades tecnológicas en el desarrollo del proceso administrativo[722]. La posibilidad de contratar y emplear el *cloud computing* tenía base en el artículo 31 de la LAE. En su primer apartado recogía que *"podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas"* , añadiendo en su apartado segundo que los documentos electrónicos que afecten a los administrados deberán conservarse en idéntico soporte, *"ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo"*, asegurándose la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. Por último, en su apartado 3, se establecían las medidas de garantías para el almacenamiento electrónico, preceptuando que *"deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados"*. Por lo tanto, se habilitaba de manera genérica la posibilidad de utilizar medios electrónicos para almacenar y tratar archivos administrativos.

Estos condicionantes en la utilización de medios electrónicos en la tarea administrativa volvían a manifestarse en la regulación del expediente electrónico. El artículo 32 de la LAE, tras definir qué es expediente electrónico y desarrollar el proceso de foliado, establecía que *"la remisión de expedientes podrá ser sustituida a todos los*

---

de abril, reguladora de las Bases del Régimen Local, reconociendo como competencias de las Diputaciones *"La prestación de los servicios de administración electrónica y la contratación centralizada en los municipios con población inferior a 20.000 habitantes"*.

[721] Sentencia del Tribunal Constitucional de 9 de junio de 2016, núm. 111/2016, FJ 11. Accesible en: http://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2016-6839.pdf. Último acceso: 08.08.2018.

[722] Además de cuestionar las capacidades personales y técnicas de las administraciones públicas en España, como, *ad supra*, hemos referenciado con ACÍN FERRER.

efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo". Por lo tanto, posibilitaba el acceso a documentos y expedientes electrónicos, así como la sustitución de los documentos físicos por formatos electrónico, si bien, no determinaba el sistema técnico en el que debe producirse dicho almacenamiento.

El informe[723], presentado el 21 de junio de 2013, sobre las reformas necesarias en las Administraciones públicas en España elaborado por la Comisión para la Reforma de las Administraciones públicas (CORA)[724], creada en 2012 para mejorar la eficiencia y eficacia de la utilidad pública, incide en las medidas para impulsar la administración electrónica, potenciando la informatización y digitalización de las relaciones, documentos y gestión administrativa. Muchas de las acciones presentadas se materializaron en la LPACAP; la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP)[725]; y la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público por la que se trasponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP)[726].

PALOMAR OLMEDA[727], estudiando la promulgación de la LPACAP y la LRJSRP, nos recuerda que *"una de sus líneas esenciales es, precisamente, el impulso a la Administración electrónica hasta el punto de convertir dicho impulso en una obligación de la Administración que los ciudadanos pueden exigir"*. Este impulso, como posteriormente veremos, determina como habitual proceder el medio electrónico. Este nuevo funcionamiento exige una serie de actuaciones políticas, técnicas y organizativas que deben desarrollarse en la normativa de referencia. La incorporación del contenido de

[723] Se puede acceder al informe completo en: https://administracion.gob.es/pag_Home/dam/jcr:4c4e8573-6220-4b6a-9397-8f95e566b42a/INFORME-LIBRO.pdf. Último acceso: 08.08.2018.

[724] Sobre la CORA: http://www.sefp.minhafp.gob.es/web/areas/reforma_aapp.html. Último acceso: 08.08.2018.

[725] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566. Último acceso: 08.08.2018.

[726] Accesible en: https://www.boe.es/boe/dias/2017/11/09/pdfs/BOE-A-2017-12902.pdf. Último acceso: 08.08.2018.

[727] PALOMAR OLMEDA, Alberto: "El paradigma del cambio: la transformación tecno", *Actualidad Jurídica Aranzadi,* 2016, Cizur Menor, núm. 920/2016, parte Tribunal. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

la LAE y de su Reglamento de desarrollo[728], potenciando los medios electrónicos como preferentes en las comunicaciones y gestión administrativa, facilita la adopción de las medidas oportunas. Por otra parte, el derecho de los ciudadanos, personas físicas, a comunicarse a través de los medios electrónicos con las Administraciones públicas aparece reconocido en el artículo 14 de la LPACAP, introduciendo, como novedad, la obligatoriedad de la utilización de este medio para los profesionales que requieran colegiación obligatoria para los trámites realizados, en razón de su actividad profesional, con las Administraciones públicas, así como para los empleados de las Administraciones públicas *"para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público"*[729].

La normalización de los medios electrónicos en la gestión administrativa queda patente en la Exposición de Motivos de la LPACAP, estableciendo, EM III, que *"en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las Administraciones"*, evolución necesaria frente al dictado establecido por la LAE. Esta tramitación electrónica obliga a dotar de una serie de herramientas que permitan a las Administraciones cumplir con los dictados que marca la Ley: los registros electrónicos de apoderamientos, artículo 6, deben ser *"plenamente interoperables"* entre las distintas administraciones territoriales; los sistemas de identificación de los interesados, artículo 9, deben facultar a los administrados a realizar el procedimiento a través de canales electrónicos; los registros de funcionarios habilitados, artículo 12, deben ser *"plenamente interoperables"* e *"interconectados con los de las restantes Administraciones Públicas"* para el auxilio en la identificación o firma regulada en la LPACAP; y la práctica de las notificaciones, de manera preferente y en todo caso cuando así lo solicite el interesado, debe realizarse por medios electrónicos, artículo 41.

---

[728] Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2009-18358. Último acceso: 08.08.2018.

[729] El artículo 14.2 establece los sujetos obligados a relacionarse a través de los medios electrónicos en el procedimiento administrativo. Si bien, excepciona la obligación en su apartado 3, cuando las administraciones establezcan *"la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios"*. Exige regulación reglamentaria, cuando la LAE imponía rango legal. El dictado del artículo podría ampliar los sujetos obligados a realizar las comunicaciones a través de medios electrónicos.

Mención especial requiere el sistema de registros y archivos de documentos, artículos 16 y 17. La normativa obliga a un registro electrónico general para cada Administración y organismo público o entidad vinculada o dependiente, debiendo, en el caso de estos últimos, ser *"plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende"*. La entrada de un documento en formato papel, por los interesados, debe ser digitalizada en las oficinas de asistencia, anotándose en la Administración u organismo correspondiente. Relacionada con esta obligación se vincula el precepto sobre el archivo de documentos, *"cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados"*. El formato deberá garantizar *"la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión"*. La configuración de un archivo digital único, en palabras de BUSTOS[730], es la prueba de fuego de la administración sin papeles.

Los requisitos de interoperabilidad, de capacidad para adaptarse a la demanda de espacio, de acceso desde diferentes localizaciones y la posibilidad de actuar bajo un *software* común en las administraciones de acceso, disponible en red, son características que definen al *cloud computing*. La obligación del archivo único y la generalización de la tramitación de los procedimientos por medios electrónicos, debiendo garantizar la autenticidad, integridad y conservación de los documentos, permite solventar, ante herramientas como la nube, los problemas de espacio, físico e informático, y el descontrol documental que se viene produciendo en algunas administraciones. Herramienta que también posibilita una consulta posterior de forma independiente de la información y documentos almacenados en la nube. Hay que tener presente que el artículo 28.2 de la LPACAP establece que los interesados no están obligados a aportar documentos ya elaborados por cualquier administración, documentos originales[731] o ya aportados con anterioridad. Esta facultad que se establece para los interesados es fácilmente configurable en un entorno con nube interoperable.

---

[730] BUSTOS, Gerardo: "Seis obligaciones básicas en el nuevo funcionamiento electrónico de las administraciones públicas", *Actualidad Jurídica Aranzadi,* 2016, Cizur Menor, núm. 923/2016, parte Comentario. Acceso a través del servicio digital Thomson Reuters Proview (bajo suscripción).

[731] *"…salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario…"*.

La configuración de la nube permite, de manera complementaria, cumplir con los principios generales que recoge la LRJSRP[732]. Implantar una herramienta colaborativa como la nube haría cumplir el propósito del artículo 157 de la LRJSRP, que impone la reutilización de sistemas y aplicaciones de propiedad de la Administración[733]. Precepto que se complementa con la previsión de transferencia tecnológica entre Administraciones, artículo 158, por el cual las Administraciones mantendrán directorios actualizados de aplicaciones para su libre reutilización, debiendo ser debidamente interoperables con el directorio general establecido en la Administración General del Estado[734].

Muchas Administraciones públicas, sobre todo aquellas entidades locales menores, pueden tener dificultades, como ya se ha indicado, para contratar y gestionar herramientas informáticas como el *cloud computing*. Consciente de las dificultades, la Disposición adicional segunda de la LPACAP posibilita a que las comunidades autónomas y las entidades locales puedan adherirse a las plataformas y registros que la Administración General del Estado facilita en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico. *Ad supra* se señaló que las Diputaciones provinciales ostentan las competencias de prestación de los servicios electrónicos, para la administración electrónica, en las entidades locales de menos de 20.000 habitantes.

Recientemente se ha promulgado la LCSP, en vigor desde el 9 de marzo de 2018, que potencia la innovación tecnológica en la contratación pública. Aunque el objeto de

---

[732] Artículo 3.2: *"Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados".*

[733] Expresamente declara el artículo 157.1: *"Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas".*

[734] Estos no son los únicos preceptos en los que la LRJSRP regula los medios electrónicos. El Capítulo V ordena el funcionamiento electrónico del sector público (artículos 38 a 46), preceptos de carácter básico, que, en términos generales, se pronuncian en similares términos a lo establecido en la LPACAP, principalmente en el archivo electrónico de documentos (artículo 46) y en la exigencia de interoperabilidad.

regulación sea especial, debemos reseñar, aunque sea en unas breves notas, la influencia de la norma en el empleo de los medios electrónicos como proceder básico para la contratación en las Administraciones públicas.

El tiempo que transcurre entre el inicio y la adjudicación en los procedimientos de contrataciones en las Administraciones públicas en España es excesivamente dilatado[735], lo que se traduce en una ineficiencia en la gestión administrativa, por no cubrir las necesidades que la contratación requiere en el menor tiempo posible y por los costes económicos que supone eternizar los procedimientos de contratación pública[736]. Estos argumentos justifican una reforma en el procedimiento de contratación pública, empleando herramientas que redunden en una mayor eficacia. La propia Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE[737] señala, considerando 52, que *"*(los medios electrónicos) *deben convertirse en el método estándar de comunicación e intercambio de información en los procedimientos de contratación, ya que hacen aumentar considerablemente las posibilidades de los operadores económicos de participar en dichos procedimientos en todo el mercado interior"*. En este sentido, VALERO TORRIJOS[738] expone que las normas comunitarias en la materia han tenido por objeto, principalmente, crear las condiciones jurídicas que faciliten la creación

[735] La Comisión Europea estimó que el tiempo medio entre la convocatoria de la licitación y la adjudicación era de 108 días, media de la Unión. Sin embargo, en el caso de España se cifra en 117 días. COMISIÓN EUROPEA - COMMISSION STAFF (WORKING PAPER): "Evaluation Report Impact and Effectiveness of EU Public Procurement Legislation", 2011, part 1, p.117-118. Accesible en: https://ec.europa.eu/docsroom/documents/15468/attachments/1/translations/en/renditions/pdf. Último acceso: 08.08.2018.

[736] El coste económico del proceso de adquisición representa un alto porcentaje del contrato, entre un 18% y un 19%. COMISIÓN EUROPEA - COMMISSION STAFF (WORKING PAPER): "Evaluation Report Impact and Effectiveness of EU Public Procurement Legislation", 2011, part 1, p. xvii. Accesible en: https://ec.europa.eu/docsroom/documents/15468/attachments/1/translations/en/renditions/pdf. Último acceso: 08.08.2018.

[737] Accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2014.094.01.0065.01.SPA. Último acceso: 08.08.2018.

[738] VALERO TORRIJOS, Javier: "Una lección del pasado: los problemas e insuficiencias derivados de las opciones de transposición por parte del legislador español", *La transposición en España de la normativa europea sobre contratación pública electrónica: una oportunidad para la innovación tecnológica,* 2015, La Nueva Contratación Pública, p. 36-37. Accesible en: http://www.obcp.es/index.php/mod.documentos/mem.descargar/fichero.documentos_La-nueva-contratacion-publica_e813ae7b%232E%23pdf/chk.cdd19408e57c2bf2e92eb186d7786d1b. Último acceso: 08.08.2018.

de un mercado europeo en la contratación pública, sin embargo, las normas estatales en materia de contratación, hasta la fecha, no han desarrollado un modelo propio de contratación pública, adaptado a las particularidades políticos-administrativas, en el que los medios electrónicos jueguen un papel transformador.

La contratación pública electrónica debe insertarse dentro del concepto de administración pública electrónica, entendida como la utilización de las TIC para esta tarea administrativa[739]. La contratación pública electrónica pretende, en última instancia, la sustitución de los canales habituales de la administración por medios simplificados que empleen instrumentos electrónicos[740]. Estos medios electrónicos deberán respetar las características que dictan las DA 16ª y 17ª de la LCSP. En las notificaciones y comunicaciones de la tramitación de la adjudicación, procedimiento, del contrato; en la presentación de ofertas y solicitudes de participación; y en el recurso especial, los medios electrónicos juegan un papel esencial, a pesar de las múltiples excepciones que la propia Ley adopta.

La obligatoriedad en la utilización de los medios electrónicos que establece el artículo 22 de la Directiva 2014/24/UE[741] no encuentra reflejo en la LCSP, que relega la regulación genérica de los medios de comunicación de la administración para la contratación pública a la DA 15ª, *"las notificaciones a las que se refiere la presente Ley se podrán realizar mediante dirección electrónica habilitada o mediante comparecencia electrónica"*. El empleo optativo de estos medios se encuentra restringido, considerando los medios electrónicos como exclusivos, como hemos indicado, en *"la práctica de las notificaciones y comunicaciones derivadas"* de la tramitación de los procedimientos de

[739] MARTÍNEZ GUTIÉRREZ, Rubén: "El uso de los medios electrónicos en la contratación pública. La relación entre las Leyes 39 y 40 de 2015 y las Directivas 24 y 55 de 2014 de contratación pública y facturación electrónica. Propuestas para tu transposición", *La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho*, 2017, INNAP Investiga, p.286.

[740] Para saber más sobre la contratación pública electrónica léase *Libro verde sobre la generalización del recurso a la contratación pública electrónica en la UE*, 2010, 571 final, de 18 de octubre de 2010, accesible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52010DC0571; y *Contratación pública electrónica de extremo a extremo para modernizar la administración pública*, 2013, 0453 final, de 26 de junio de 2013, accesible en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52013DC0453. Últimos accesos: 08.08.2018.

[741] *"Los Estados miembros garantizarán que todas las comunicaciones y todos los intercambios de información en virtud de la presente Directiva, y en particular la presentación electrónica de ofertas, se lleven a cabo utilizando medios de comunicación de conformidad con los requisitos establecidos en el presente artículo…"*.

adjudicación de contratos (DA 15ª.2) y en *"la presentación de ofertas y solicitudes de participación"* (DA 15ª.3). Esta obligatoriedad del empleo de los medios electrónicos, informáticos y telemáticos tiene, sin embargo, excepciones que pueden hacer decaer uno de los motivos principales expuestos para la promulgación de la nueva Ley de contratos y, además, contravenir los dictámenes de la normativa europea. No debe olvidarse la disparidad que puede surgir con la LPACAP y, en menor medida, con la LRJSRP, que contienen disposiciones de carácter básico.

A pesar de esta crítica, sí ha supuesto una evolución en la instrumentación de los medios electrónicos como herramienta de trabajo y comunicaciones en las Administraciones públicas. El establecimiento del documento europeo único de contratación (DEUC), artículo 140.1, a pesar de que puede ser presentado en formato papel; la utilización de la red e-Certis por el Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público como base de datos que contiene información relevante de acreditación de la solvencia y aptitud de los empresarios, DA 35ª y artículo 87.2; los sistemas dinámicos de adquisiciones, regulado en los artículos 223 a 226, y definido en la LCSP como *"proceso totalmente electrónico, con una duración limitada y determinada en los pliegos, y debe estar abierto durante todo el período de vigencia a cualquier empresa interesada que cumpla los criterios de selección"*; la subasta electrónica, artículo 143, aunque no se contemple como sistema de contratación pública obligatoria en algunos procedimientos[742]; la consolidación de la factura electrónica; y el establecimiento del procedimiento abierto simplificado, artículo 159, que concibe, entre otras obligaciones en el empleo de los medios electrónicos, que *"toda la documentación necesaria para la presentación de la oferta tiene que estar disponible por medios electrónicos desde el día de la publicación del anuncio en dicho perfil de contratante"*, tienen como finalidad mejorar la eficiencia de las Administraciones públicas a través de las TIC.

Sin lugar a dudas, el empleo del *cloud computing* en las Administraciones públicas permitirá la necesaria intercomunicación entre administraciones y entre administraciones

[742] En la discusión sobre la futura Ley de contratos, MARTÍNEZ GUTIÉRREZ consideraba a la subasta electrónica como medio obligatorio de utilización ante los contratos menores. MARTÍNEZ GUTIÉRREZ, Rubén: "El uso de los medios electrónicos en la contratación pública. La relación entre las Leyes 39 y 40 de 2015 y las Directivas 24 y 55 de 2014 de contratación pública y facturación electrónica. Propuestas para tu transposición", *La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho*, 2017, INNAP Investiga, p.316-317.

y administrados, clave para un servicio público eficiente. Por lo tanto, para poder implantar la administración electrónica, se hace necesario emplear herramientas que garanticen la interoperabilidad entre las distintas plataformas tecnológicas y sistemas utilizados por todos los sujetos relacionados. La nube, con la posibilidad de implantar sistemas *PaaS* y *SaaS*, puede homogenizar los servicios y procedimientos electrónicos. Garantizar la integridad de los datos alojados y en tránsito acaece, igualmente, como requisito indispensable para la utilización de los medios electrónicos.

Con las consideraciones anteriores, ya sea para un modelo *cloud* u *on premise*, no es cuestionable el respeto a los límites establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad[743] (ENS) y el Real Decreto 4/2010, de 8 de enero, que aprueba el Esquema Nacional de Interoperabilidad[744] (ENI), prevenciones de obligado cumplimiento en el seno de la administración electrónica. Por lo tanto, el centro neurálgico de este estudio será determinar si es posible contratar los servicios de computación en la nube, no tanto por la operatividad técnica del servicio, sino por la externalización[745] de las actuaciones que hasta la fecha han quedado dentro del ámbito de actuación de las Administraciones públicas. Antes de avanzar, se deben describir las directrices que el ENS y el ENI imponen para la implantación de tecnologías de la información, centrándonos siempre en aquellos aspectos que tienen incidencia en la relación contractual.

El Esquema Nacional de Seguridad incide de manera constante en una serie de aspectos[746]:

- La implantación del *cloud computing* en las Administraciones públicas debe ser objeto de un análisis de riesgos, sobre la base de la sensibilidad de los datos y el nivel de amenaza. Este análisis determinará el modelo más

[743] Accesible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330. Último acceso: 08.08.2018.

[744] Accesible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1331. Último acceso: 08.08.2018.

[745] Aunque la externalización no es una de las características esenciales del *cloud*, sí es un rasgo diferenciador al considerarse un servicio de pago por demanda. Véase "definición y características", Capítulo I.a. Cuando la contratación la realiza un ente público, podría cuestionarse esta particularidad, si bien, como posteriormente veremos, suele acudirse a proveedores de servicios implantados en el mercado.

[746] Se recomienda leer AEPD: "Guía para clientes que contraten servicios de Cloud Computing", 2018, p. 19-23. Accesible en: https://www.aepd.es/media/guias/guia-cloud-clientes.pdf. Último acceso: 08.08.2018.

oportuno y los controles y salvaguardas que deben realizarse para disminuir los riesgos hasta un nivel considerable.

- La seguridad debe ser llevada a cabo por personal cualificado, abarcando las tareas de prevención, revisión y auditoría. Con el Reglamento General de Protección de Datos de la Unión Europea será el delegado de protección de datos el encargado de supervisar el cumplimiento de la normativa[747].
- Se exigen técnicas de cifrado para los datos que están en tránsito y aquellos que se encuentran almacenados, con el fin de garantizar la correcta confidencialidad. La justificación se basa en la especial sensibilidad de los datos tratados por las Administraciones públicas. Esta garantía se complementa con la realización de copias de respaldo que aseguren la disponibilidad e integridad de los datos almacenados ante cualquier incidente.
- Se deben establecer los mecanismos que garanticen la continuidad del servicio en el supuesto de catástrofes o incidentes severos, para lo que se requiere un sistema de gestión de incidencias de seguridad acorde con el nivel de servicios exigidos.
- La implantación del *cloud computing* exige cumplir con las exigencias del artículo 34 del ENS, que establece la obligatoriedad de realizar auditorías de seguridad ordinarias y extraordinarias. Las auditorías ordinarias se realizarán de forma regular al menos cada dos años, y las extraordinarias siempre que se produzcan modificaciones sustanciales en los sistemas de información que puedan repercutir en las medidas de seguridad. Estas auditorías extraordinarias determinarán la fecha de cómputo para el cálculo de los dos años establecidos para la realización de la siguiente auditoría regular ordinaria.

Aunque aquí solo hemos resaltado aspectos que repercuten de forma directa en las cláusulas contractuales que deben regir en la prestación del servicio, el ENS contempla los requisitos específicos, los métodos de trabajo, la conducta utilizada, los criterios metodológicos y los requisitos en la realización de las auditorías (método, destinatarios y

[747] Al respecto, la AEPD ha recogido en un documento los aspectos esenciales del delegado de protección de datos en las Administraciones públicas. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: "El Delegado de Protección de Datos en las Administraciones Públicas", 2017. Accesible en: https://www.aepd.es/media/docs/funciones-dpd-en-aapp.pdf. Último acceso: 08.08.2018.

conclusiones) para una correcta evaluación, mantenimiento, previsión y revisión de la administración electrónica.

Respecto a las exigencias que establece el Esquema Nacional de Interoperabilidad, debemos resaltar las siguientes:

- Los documentos y servicios de la administración electrónica puestos a disposición de otras instituciones del sector público o de la ciudadanía en general deben estar disponibles mediante estándares abiertos. Debe garantizarse los principios de neutralidad tecnológica, siendo accesibles y funcionales con independencia de la elección tecnológica del ciudadano.
- Para garantizar la recuperación y conservación de los documentos electrónicos en el desarrollo de la actividad administrativa deben adoptarse medidas organizativas y técnicas necesarias para afianzar la interoperabilidad.
- Se debe garantizar la conservación de los documentos electrónicos en el formato en que hayan sido elaborados, enviados o recibidos, preferentemente en un formato con estándar abierto que preserve la integridad del documento, de la firma electrónica y los metadatos que lo acompañan.

Estas directrices del ENI pretenden garantizar la portabilidad de los datos ante un cambio en el proveedor de servicios, salvaguardando el derecho de los ciudadanos al acceso a los mismos y fomentando el uso de estándares abiertos.

Mejora en la gestión administrativa, transparencia y participación e interconexión administrativa, bajo el paraguas de la seguridad técnica en la información y datos utilizados, son las razones principales para el empleo de los medios electrónicos en las Administraciones públicas.

b. Tipo contractual del cloud computing según la normativa administrativa.

La falta de un marco jurídico e institucional que regule la contratación de la computación en la nube, consecuencia del principio de neutralidad tecnológica, para las Administraciones públicas dificulta determinar el tipo contractual de la herramienta electrónica en el sector público. Aunque las dificultades relacionadas con la inexistencia de un marco jurídico y un organismo prescriptor tienen mayor relevancia en la implantación de los servicios en la nube de las Administraciones de ámbito estatal y

autonómico, por el volumen de datos tratados y los requisitos de interoperabilidad con otras instituciones, la diversidad e incompatibilidad normativa afecta a todas las Instituciones públicas[748].

Determinado el ámbito de aplicación y subjetivo de la LCSP, artículos 2 y 3, la delimitación de los tipos contractuales que establece la Ley fijará la viabilidad de someter los servicios de computación en la nube al contenido prestacional de los contratos regulados en la normativa. Dos contratos típicos pueden establecer el régimen prestacional del *cloud computing*: el contrato de suministro y el contrato de servicios.

Partiendo de la regulación del contrato de suministros en el artículo 16 de la LCSP[749], el encuadre legal de la nube en esta tipología de contratos vendría por la consideración expuesta en apartado 3.b del artículo *"…adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información…"*, si bien, el legislador, conociendo de las novedades y la innovación producidas en las nuevas TIC podría haber introducido nuevos medios electrónicos o aclarado las características de los mismos y no replicar, a estos efectos, la antigua redacción del artículo 9 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la

[748] Instituto Nacional de Tecnologías de la Comunicación (INTECO): "Estudio sobre el *cloud computing* en el sector público en España", 2012, p. 90-100. Accesible en: https://www.scribd.com/document/99564543/Estudio-sobre-cloud-computing-en-el-sector-publico-en-Espana. Último acceso: 08.08.2018. INTECO ahora es el Instituto Nacional de Ciberseguridad (INCIBE).

[749] El artículo 16 de la LCSP establece: *"1. Son contratos de suministro los que tienen por objeto la adquisición, el arrendamiento financiero, o el arrendamiento, con o sin opción de compra, de productos o bienes muebles.*
2. Sin perjuicio de lo dispuesto en la letra b) del apartado 3 de este artículo respecto de los contratos que tengan por objeto programas de ordenador, no tendrán la consideración de contrato de suministro los contratos relativos a propiedades incorporales o valores negociables.
3. En todo caso, se considerarán contratos de suministro los siguientes:
a) Aquellos en los que el empresario se obligue a entregar una pluralidad de bienes de forma sucesiva y por precio unitario sin que la cuantía total se defina con exactitud al tiempo de celebrar el contrato, por estar subordinadas las entregas a las necesidades del adquirente.
b) Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos, en cualquiera de sus modalidades de puesta a disposición, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios.
c) Los de fabricación, por los que la cosa o cosas que hayan de ser entregadas por el empresario deban ser elaboradas con arreglo a características peculiares fijadas previamente por la entidad contratante, aun cuando esta se obligue a aportar, total o parcialmente, los materiales precisos.
d) Los que tengan por objeto la adquisición de energía primaria o energía transformada".

Ley de Contratos del Sector Público[750] (TRLCSP). PALOMAR OLMEDA[751], teniendo como referencia el TRLCSP, consideraba que la definición general del contrato de suministro podría encajar con la prestación de servicio de computación en la nube, por cuanto podría tratarse de un supuesto de arrendamiento, con o sin opción de compra, de un producto. Vista la delimitación conceptual del contrato de suministro, y su posible acomodo con el contrato de prestación de servicios de *cloud computing,* es oportuno realizar un estudio del esquema jurídico para confirmar que las características propias del contrato de computación en la nube se adecúan al dictado de la regulación del contrato de suministro.

El artículo 298 de la LCSP regula el arrendamiento, estableciendo las obligaciones del empresario titular del contrato, asumiendo durante el plazo de vigencia del contrato la obligación de mantener el objeto. Es complejo, a priori, en un sistema de *cloud computing* determinar la capacidad puesta a disposición de las Administraciones públicas. Las certificaciones podrían instaurarse como instrumento garante de la efectiva puesta a disposición del contratante, en cuanto al volumen suficiente de espacio de almacenamiento en el tiempo y cantidad determinada.

Más complejo es adecuar la regulación sobre la ejecución de los contratos de suministros a la realidad de la nube, principalmente en cuanto a la entrega y recepción, artículo 300 de la LCSP, y respecto a las facultades de inspección de la administración en el proceso de fabricación, artículo 303 de la LCSP. La configuración del *cloud* no reúne las características propias de un dispositivo para el tratamiento de la información[752], que, si bien no lo define la norma, atendiendo al concepto jurídico tradicional[753], no consume

[750] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2011-17887. Último acceso: 08.08.2018.

[751] PALOMAR OLMEDA, Alberto: "Incidencia del cloud computing en el ámbito de la contratación pública", *Derecho y cloud computing*, 2012, p. 211.

[752] El artículo 16.3.b) de la LCSP establece que se considerará contrato de suministro: *"Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos, en cualquiera de sus modalidades de puesta a disposición, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios"*.

[753] El derogado Real Decreto Legislativo 2/2000, de 16 de junio, por el que se aprueba el texto refundido de la Ley de Contratos de las Administraciones Públicas establecía en el artículo 173, dentro de las normas generales del contrato de suministro, que se entenderá por tratamiento de la información y telecomunicaciones:

un producto disponible en y para el mercado con características genéricas. No hay un proceso informático de transformación configurado de forma específica para el uso de las Administraciones públicas, en todo caso, ese proceso será realizado por los programas informáticos o por la tarea de programación que puede ser ejecutada en el entorno de la nube.

Por lo expuesto, podemos concluir que el régimen jurídico establecido en la LCSP para el contrato de suministro, aunque a priori pudiera considerarse como la figura jurídica más oportuna para regular el contrato de la nube con las Instituciones públicas, no se adapta a los rasgos definitorios de la herramienta informática. Dos características condicionan su aplicabilidad: en primer lugar, la determinación del *cloud computing* como un servicio de carácter general, que impide la aplicación de la regulación de la entrega y recepción de los bienes objeto de suministros establecidos en la LCSP; así como, en segundo lugar, las inservibles facultades de inspección adjudicadas a las Administraciones públicas por la Ley debido al marco donde se desarrolla la prestación del servicio de computación en la nube. A estos dos condicionantes que dificultan la concepción del contrato de *cloud* como contrato de suministros debemos añadir la no adecuación de la herramienta al concepto tradicional de entrega de suministro. En consecuencia, el marco jurídico del contrato de suministro no es válido para la computación de la nube, siendo necesaria una reconsideración de la configuración, es decir, una modificación del régimen jurídico del contrato de suministros para adaptarlo a las TIC. No parece, sin embargo, la voluntad del legislador acoger la propuesta planteada, al reproducir en la nueva LCSP lo establecido en el TRLCSP.

El contrato de servicios se plantea como el marco jurídico aplicable para la prestación de la nube cuando no encuentra conciliación jurídica con el contrato de suministros, más si cabe ante herramientas que plantean nuevos procesos tecnológicos basadas en la información y comunicación.

"…a) Por equipos para el tratamiento de la información, las máquinas o conjuntos de máquinas y dispositivos, interconectados o no, capaces de realizar las operaciones necesarias para preparar la utilización de la información a fines determinados…
d) Por sistemas para el tratamiento de la información, los sistemas compuestos de equipos y programas capaces de realizar las funciones de entrada, proceso, almacenamiento, salida y control de la información, con el fin de llevar a cabo una secuencia de operaciones con datos…"
Accesible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2000-11533. Último acceso: 08.08.2018.

El artículo 17 de la LCSP sigue definiendo el contrato de servicios en un sentido negativo, cuando el contrato no sea considerado obra o suministro[754]. El TRLCSP establecía idéntica definición, si bien, añadía *"los contratos de servicios se dividen en las categorías enumeradas en el Anexo II"*. El citado Anexo II configuraba un listado de categorías, clasificando a los contratos de servicios, apareciendo en la séptima categoría los *"servicios de informáticas y servicios conexos"*. Esta aproximación a la conveniencia de considerar al *cloud computing* como un contrato de servicio no aparece en la nueva redacción de la normativa. Será necesario, por tanto, ahondar en el régimen jurídico establecido en la LCSP y reflexionar sobre su similitud con los servicios establecidos en la Ley.

El contenido y los límites de los contratos de servicios se recogen en el artículo 308 de la LCSP. A los efectos de estudiar la viabilidad de la computación en la nube como servicio, los apartados .1 y .3 son especialmente relevantes. El primero de ellos determina que, salvo que en las cláusulas administrativas o el documento contractual se establezca lo contrario, los productos protegidos con propiedad intelectual o industrial llevarán aparejados la cesión de estos derechos a la administración. Señala que, incluso en el contrato en el que se excluya la cesión de los derechos de propiedad intelectual, el órgano de contratación podrá siempre autorizar el uso del producto a los entes, organismos y entidades del sector público. La importancia del citado precepto radica en la dispar ordenación de los derechos de propiedad intelectual e industrial que puede darse en la contratación en la nube. Como ya indicáramos cuando explicábamos las características de la computación en la nube, depende del proveedor de servicios con el que se establezca la relación contractual, así como de la implantación del modelo de *cloud*, los derechos citados se cederán o no a los clientes, en este caso a la Administración. De ahí que resulte vital la salvaguarda que establece el precepto, al regular la posible exclusión de la cesión de los citados derechos, si bien la Administración conserva la potestad de autorizar el uso a los diferentes sujetos del sector público. De esta manera, las Administraciones públicas pueden establecer relaciones contractuales con un amplio abanico de proveedores del servicio, favoreciendo la contratación con entidades de ámbito internacional propias del sector y de los servicios demandados.

[754] El artículo 17 de la LCSP, de forma literal, recoge: *"Son contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o suministro, incluyendo aquellos en que el adjudicatario se obligue a ejecutar el servicio de forma sucesiva y por precio unitario"*.

Importante es la redacción del apartado .3, no porque sea directamente aplicable, sino porque recoge la posibilidad de definir, en función de la evolución y las circunstancias, el concreto servicio. Para *"los contratos de servicios que impliquen el desarrollo o mantenimiento de aplicaciones informáticas"* la definición del objeto puede completarse con la referencia a las funcionalidades a desarrollar, *"sin perjuicio de que puedan concretarse dichas funcionalidades por la Administración atendiendo a consideraciones técnicas, económicas o necesidades del usuario durante el período de ejecución…"*. Este apartado, introducido en la nueva redacción de la Ley, aunque lo delimite solo a algunos servicios informáticos, tiene presente la dificultad de definir las prescripciones técnicas de forma inicial por el contratante, problema reiterado cuando se pretende contratar los servicios del *cloud computing*, recurriendo comúnmente a las certificaciones, incluso permitiendo la flexibilidad en la implementación del servicio.

Por lo tanto, aunque la LCSP no recoja en la definición del contrato de servicios la posible adecuación de este desarrollo informático, consecuencia de la redacción en sentido negativo del término y de la eliminación de la clasificación establecida en el Anexo II del TRLCSP, las posibilidades que plantea, por analogía, el apartado 308.3 de la LCSP permiten considerar que el régimen jurídico del contrato de servicios es el más adecuado para la regulación del *cloud computing* cuando contrata el sector público, siempre y cuando no constituya, por sus propias características, un suministro. Por consiguiente, la prestación de servicios de computación en la nube puede configurarse como un contrato de servicios típico, donde los pliegos de las cláusulas administrativas y técnicas del contrato regirán las obligaciones sustantivas concernientes al proveedor de servicios.

c. Cláusulas necesarias en el contrato administrativo.

Independientemente del tipo contractual, será el pliego de cláusulas administrativas particulares y de prescripciones técnicas los que delimitarán si el contenido obligacional de las partes cumple los dictámenes de la contratación administrativa. La complejidad radica en el modelo de negocio de los proveedores del *cloud*, copado por proveedores internacionales donde el "lo tomas o lo dejas" supone el punto de partida de las negociaciones. Aspectos como el pago por el uso o el dimensionamiento dinámico del servicio en función de la demanda, características que exigen contratos flexibles, condicionan el encuadre en el marco regulador estudiado, aunque la LCSP mejore, como se ha puesto de manifiesto, el corsé establecido con el TRLCSP, exigiendo unos pliegos

adaptados a la contratación de la herramienta informática y gestionados con unidades de fiscalización e intervención.

Es primordial el estudio de los riesgos inherentes a la implantación de los servicios del *cloud* en las Instituciones públicas para determinar las cláusulas administrativas que deben recoger los pliegos administrativos[755]. MANUEL MARTÍNEZ[756] argumenta que, decidido el tipo de servicio y los servicios concretos a migrar, hay que hacer un análisis de los riesgos inherentes a la implantación, dado que ninguna Administración pública ha considerado esta forma de provisión de servicios en sus planes de seguridad ni de adaptación al ENS. Para ver la importancia de la contratación de las TIC en el sector público, un dato relevante puede ser el importe total de licitaciones, en términos económicos, de estas tecnologías: 1.735.897.609 € en el primer semestre del año 2017[757].

Analizando los riesgos contractuales, se propone:

- El respeto a la normativa de protección de datos personales debe estar presente en la redacción de los contratos administrativos. Se debe actuar con especial cautela cuando el proveedor de los servicios se encuentre fuera de España o un país con equivalente protección, debiendo atender a los dictámenes establecidos en la Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, del Parlamento Europeo y del Consejo cuando el proveedor no se encuentre radicado en los citados países. El RGPD sigue el modelo establecido por la Directiva 95/46[758].

[755] Aunque muchos de los riesgos del *cloud computing* aquí señalados son comunes a la relación que mantienen los proveedores con las empresas y con los consumidores y usuarios, resultan de especial relevancia citarlos dada la posición que ocupan las Administraciones públicas con sus administrados.

[756] MARTÍNEZ, Manuel: "Cloud computing y la Administración Pública", *Boletic*, 2011, nº 60, p. 47-49 http://www.astic.es/sites/default/files/boletic_completos/boletic_60_completo.pdf. Último acceso: 08.08.2018.

[757] ADJUDICACIONES Y LICITACIONES TIC: "Barómetro Inversión del Sector Público – Informe Semestral", 2017, 1er Semestre 2017, p. 3. Accesible en: http://www.adjudicacionestic.com/front/articulo-contenido.php?id=129 (bajo registro). Último acceso: 08.08.2018.

[758] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: "Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento", 2017, p. 28. Accesible en:

- Relacionado con el punto anterior, las Instituciones públicas deben conocer la ubicación de los datos, determinando la posible subcontratación o no de los servicios y sus facultades de intervención ante la subcontratación. Como indica la Agencia Española de Protección de Datos[759], la posibilidad del tratamiento de datos fuera del territorio nacional, característica del *cloud computing*, constituye un elemento de especial relevancia en el caso de las Administraciones públicas. En este sentido, hay que tener en cuenta que la normativa que regula los movimientos internacionales de datos es aplicable tanto a entidades privadas como públicas. El principal problema se plantea al considerar qué autoridades competentes de terceros países podrían solicitar y acceder a datos alojados en su país, datos de los que son responsables las Administraciones públicas españolas, sin que ni siquiera se le informe de tal circunstancia. De ahí que se deba conocer y exigir al proveedor en todo momento la información de dónde van a ser tratados los datos, los requerimientos necesarios y las decisiones que puede tomar al respecto la administración encargada. No puede olvidarse que la contratación de los servicios de *cloud* por las Instituciones del sector público requiere la formalización de un contrato, conforme al artículo 12 de la LOPD[760] y los artículos de 20 a 22 del RLOPD[761].
- Las Instituciones deben garantizar, a través de las cláusulas que incorporen en el pliego, que el proveedor del servicio establezca las herramientas necesarias para que los administrados puedan ejercer su derecho de acceso a

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf. Último acceso: 08.08.2018.

[759] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: "Guía para clientes que contraten servicios de Cloud Computing", 2018, p. 18-23. Accesible en: https://www.aepd.es/media/guias/guia-cloud-clientes.pdf. Último acceso: 08.08.2018.

[760] El artículo 73.k del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, hecho público el 24 de noviembre de 2017, aunque ha recibido más de 369 enmiendas, establece como infracción grave *"encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679"*. Accesible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF. Último acceso: 08.08.2018.

[761] Se aconseja la lectura de AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento", 2017. Accesible en: https://www.aepd.es/media/guias/guia-directrices-contratos.pdf. Último acceso: 08.08.2018.

la información pública, implantando las restricciones y medidas de seguridad necesarias en aquellos datos limitados o restringidos por la normativa.

- Dentro de las herramientas informáticas que poseen las Instituciones públicas, debe manifestarse expresamente en el contrato las actuaciones permitidas y lícitas ante los derechos de propiedad intelectual e industrial, así como los derechos inherentes a las nuevas actuaciones desarrolladas al amparo del contrato de computación en la nube.
- En los pliegos administrativos debe optarse por estándares abiertos o que, al menos, posibiliten que las Instituciones no se encuentren limitadas a un operador de servicios concreto, buscando la interoperabilidad dentro de los diferentes departamentos de la Administración, así como con otras Administraciones, mitigando los posibles efectos *lock-out* presentes o futuros de un cambio de proveedor. Estos criterios técnicos deben vincularse con diferentes penalidades ante acciones que dificulten una correcta interoperabilidad.
- Es necesario determinar la disponibilidad del servicio de *cloud*, estableciendo y fijando el acceso de las Instituciones y de los administrados. Por ello, los tiempos de inactividad permisibles y las pérdidas de información aceptables, instaurando unas medidas compensatorias adecuadas ante el incumplimiento del proveedor, deben ser regulados en los contratos administrativos.
- Por los datos tratados en las Administraciones públicas, los incidentes de seguridad son el principal escollo para la administración electrónica. Tras el estudio completo de la información y datos a trasladar a la nube, se debe garantizar en el contrato el compromiso y la obligación por el proveedor del *cloud* de atender a los riesgos con celeridad, informando de forma inmediata a la administración e implementando medias preventivas[762].

[762] Reciente son las noticias sobre los fallos de LexNET que han propiciado descargas de documentos confidenciales. Entre otras noticias, PINHEIRO, Marcos: "Catalá oculta que el fallo de LexNET propició más de 400 descargas de documentos confidenciales", *eldiario.es*, 2017, noticia de 12.11.2017. Accesible en: http://www.eldiario.es/politica/Catala-descargas-ilegales-documentos-LexNET_0_706579756.html y TECNOXPLORA: "El Ministerio de Justicia denuncia al hacker que descubrió el fallo en LexNET", *laSexta.com*, 2018, noticia de 08.02.2018. Accesible en: http://www.lasexta.com/tecnologia-tecnoxplora/internet/ministerio-justicia-denuncia-hacker-que-descubrio-fallo-lexnet_20170808598994980cf2c0f4137e4fd5.html. Últimos accesos: 08.08.2018.

El estudio de las cláusulas particulares realizado cuando los contratantes son empresas o consumidores se puede replicar, en términos generales, en el análisis de las necesidades para una correcta confección del contrato administrativo. Si bien, y analizados los riesgos inherentes que supone la contratación del *cloud* cuando actúa la Administración, dos de los condicionantes presentan especiales particularidades que resultan imprescindibles discernir, y por tanto deben estar presentes en toda contratación administrativa del servicio para su correcta adecuación: la conservación de la información y los datos, de obligado cumplimiento en el ámbito administrativo; y la disponibilidad en el uso y la conservación. Volviendo a citar a MARTÍNEZ[763], el aspecto más problemático de la implantación del *cloud computing* en las Administraciones públicas es la seguridad considerada en su sentido amplio, es decir, *seguridad+disponibilidad* y *seguridad+resistencia*. Por consiguiente, el aseguramiento de la disponibilidad instantánea y la disponibilidad a medio o largo plazo son aspectos consustanciales para una correcta implantación del *cloud* en las Instituciones públicas.

La seguridad en la conservación de los datos debe observarse desde una doble perspectiva. En primer lugar, la conservación de los datos dependerá del tipo de documento, dato o información establecida en el entorno de la nube. No se puede atribuir de forma apriorística un régimen jurídico general para los expedientes administrativos, dado que cada procedimiento está determinado por la regulación sustantiva correspondiente. Sin embargo, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos[764], vigente a pesar de estar derogada la Ley que parcialmente desarrolla por la LPACAP, habilita, en el artículo 51, para que el archivo de los documentos electrónicos del expediente administrativo pueda llevarse a cabo por medios electrónicos, reconociéndose el principio de no discriminación y de equivalencia funcional. Importante es, también, la posibilidad que establece de conservar los documentos electrónicos en distintos paquetes, práctica habitual del almacenamiento en

[763] MARTÍNEZ, Manuel: "Cloud computing y la Administración Pública", *Boletic*, 2011, nº 60, p. 47-49 http://www.astic.es/sites/default/files/boletic_completos/boletic_60_completo.pdf. Último acceso: 08.08.2018.

[764] Accesible en: https://www.boe.es/buscar/act.php?id=BOE-A-2009-18358. Último acceso: 08.08.2018.

el *cloud computing*[765]. A nuestro juicio, supuso el precedente necesario para que los artículos 16 y 17 de la LPACAP, como ya se ha reseñado en el subapartado a, compelan a que cada Administración disponga de un registro electrónico general, debiendo digitalizarse los documentos presentados de manera presencial; obligando, además, a mantener un archivo electrónico único de los documentos electrónicos con los procedimientos finalizados.

El artículo 52 del RD 1671/2009 preceptúa que serán los órganos administrativos quienes dispondrán, de acuerdo con el procedimiento administrativo de que se trate, los períodos mínimos de conservación de los documentos electrónicos, pudiendo encomendarse las tareas de conversión para preservar la conservación, el acceso y legibilidad de los documentos electrónicos archivados, imponiendo la obligación de promover a los responsables de los archivos electrónicos copia auténtica, con cambio de formato, cuando no se corresponda con los formatos admitidos por el Esquema Nacional de Interoperabilidad. El precepto supone la concreción del artículo 17.2 y .3 de la LPACAP, que exige a las Administraciones garantizar que los documentos electrónicos se conserven en *"en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión"*, remarcando la posibilidad de trasladar los documentos y datos a otros formatos y soportes que garanticen la interoperabilidad entre aplicaciones. Enlazando, con la segunda perspectiva a analizar, que propugna la necesidad de emplear medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de documentos de acuerdo con el ENS.

Por lo tanto, no existe un conjunto de criterios sustantivos que, a priori, posibiliten un régimen jurídico general, dependerá del conjunto de normas que dispongan la forma, el tiempo de conservación y la disposición, entre otros, del documento o expediente administrativo.

---

[765] El artículo 51 del RD 1671/2009 establece: *"1. La Administración General del Estado y sus organismos públicos vinculados o dependientes deberán conservar en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas, que formen parte de un expediente administrativo, así como aquellos otros que, tengan valor probatorio de las relaciones entre los ciudadanos y la Administración.*
2. La conservación de los documentos electrónicos podrá realizarse bien de forma unitaria, o mediante la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos, así como para la comprobación de la firma electrónica de dichos datos."

Tratando la seguridad del *cloud computing* desde un sentido técnico, segunda perspectiva en el estudio de la seguridad en la conservación de los datos, el servicio debe cumplir con los estándares establecidos en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica. *Ad supra* se ha señalado que la administración electrónica debe cumplir con las prescripciones establecidas en el ENI y en el ENS. Profundizando y complementando lo anterior, el capítulo X del ENI regula la recuperación y conservación del documento electrónico. A los efectos de nuestros estudio, dos artículos deben ser considerados con especial cautela: el artículo 21 determina que las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en la recuperación y conservación de documentos electrónicos, delimitando y concretando tales medidas, así como estableciendo, en su apartado 2, la necesidad de crear repositorios electrónicos complementarios y equivalentes como prevención a la disponibilidad de los documentos electrónicos. Por otra parte, el precepto 22, apartados 1 y 2, exige cumplir contractualmente, respecto a los ficheros y datos, con el régimen jurídico contenido en la LOPD, por extensión también lo dispuesto en el RGPD, y el ENS, debiendo, contractualmente, garantizarse *"la integridad, autenticidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos"*. Las principales exigencias de los ENS y ENI se han expuesto al inicio del presente subapartado, dándose por reproducidas para no pecar de reiterativos.

El binomio disponibilidad-seguridad, que debe aparecer en las prescripciones técnicas del pliego administrativo y en el contrato, determinará las condiciones de uso y de conservación de los datos y la información, cláusula especialmente relevante en el ámbito administrativo ante expedientes en trámite que requieren disponibilidad en tiempo real y conservación de las condiciones de utilización. Por lo tanto, en esta regulación deben, también, las Administraciones e Instituciones públicas ser especialmente cautelosas en la redacción del expediente y la información facilitada a los licitadores, dado que regulará de forma holística las condiciones de uso y conservación, como norma sustantiva.

El INTECO[766], ahora INCIBE, proponía una serie de recomendaciones y buenas prácticas cuando el demandante del servicio de la nube es una Institución del sector público. Estas recomendaciones, unidas a las medidas preventivas y a los condicionantes esenciales estudiados, servirán de guía para la correcta aplicación del *cloud*. Partiendo del breve trazo esquemático que proponía INTECO, a continuación, formulamos y desarrollamos pautas de partida para la contratación del servicio en nube por los entes públicos[767].

La primera recomendación es implicar en la estrategia de la computación en la nube a las áreas jurídicas, tecnológicas y operativas con el fin de elaborar instrumentos contractuales que se adapten a las necesidades de la tecnología empleada. Recomendación obvia, reiterada a lo largo del análisis de las cláusulas contractuales, no solo cuando la parte contratante es la Administración. Un cambio de paradigma en las relaciones laborales y en las tareas a realizar implica un compromiso de los equipos de trabajo, que difícilmente no encontraría resistencia ni provocaría conflictos si no se aplicara una visión multidisciplinar. A partir de esta premisa, se deben acordar contratos que de forma expresa establezcan las medidas de seguridad propuestas y consensuadas, las condiciones de acceso a la información, las medidas de contingencias, las casuísticas del servicio y las condiciones de finalización del contrato y devolución de los activos y servicios contratados. Requiere que la decisión de la implantación de la nube sea una decisión y política estructural dentro del ente público. Esta concepción de política transversal aparece en las leyes LPACAP y LRJSP.

A través del contrato o mediante el ANS, las Administraciones deben garantizar que los proveedores cumplen las políticas de seguridad, siendo oportuno un proceso de evaluación mediante estándares auditables y sometiéndose a controles y revisiones de terceros que certifiquen el cumplimiento de las políticas. Dado que los proveedores pueden negarse a ser auditados, puede ser útil determinar la validez de informes de

[766] INTECO: "Estudio sobre el *cloud computing* en el sector público en España", 2012, p. 123. Accesible en: https://www.scribd.com/document/99564543/Estudio-sobre-cloud-computing-en-el-sector-publico-en-Espana. Último acceso: 08.08.2018. INTECO ahora es el Instituto Nacional de Ciberseguridad (INCIBE).

[767] No debe confundirse estas recomendaciones iniciales, que tienen como finalidad favorecer la primera toma de contacto con la herramienta y el análisis de su contratación, con los requisitos necesarios en los pliegos y contratos administrativos, analizados pormenorizadamente en páginas precedentes.

auditorías oficiales o certificaciones que garanticen niveles adecuados de calidad[768]. Esta recomendación se complementa con la garantía de realizar auditorías o certificaciones sobre la destrucción o borrado de datos, para confirmar que el proveedor realiza dichas actividades a la finalización del contrato con la Institución. La penalización ante el incumplimiento de los niveles de servicios, consignada en el contrato, debe vincularse con la obligatoriedad del proveedor de la nube de responder (responsabilidad civil) como consecuencia de su mala praxis e incumplimiento contractual, pudiendo usar como cobertura un seguro ante lo crítico del servicio y la potencial información transferida en la herramienta electrónica.

En la contratación administrativa, determinar unos niveles de servicios de forma apriorística, aunque puedan evolucionar con el desarrollo del servicio, como hemos indicado, son esenciales. La LCSP, además de regular los daños y perjuicios en los supuestos de incumplimiento parcial o defectuoso del contrato cuando no esté prevista la penalidad o que estándolo no cubriera a la Administración[769], preceptúa, en el artículo 196, la indemnización por los daños y perjuicios producidos o causados a terceros. La norma dictamina que *"será obligación del contratista indemnizar todos los daños y perjuicios que se causen a terceros como consecuencia de las operaciones que requiera la ejecución del contrato"*, salvo que sean consecuencia inmediata y directa de una orden de la Administración o tengan su origen en un vicio del proyecto elaborado por ella misma en el contrato de suministros[770]. Esta reproducción del antiguo artículo 214 del TRLCSP, impone a la Administración realizar una tarea de supervisión en los supuestos de daños o perjuicios a terceros para determinar las condiciones que motivaron los hechos, paso previo para dilucidar sobre la responsabilidad del proveedor de servicios. Por consiguiente, la responsabilidad será consecuencia solo de las actividades que constituyan el objeto del contrato. Según la tipología adoptada para el servicio de la nube, el proveedor será responsable:

[768] Ejemplo de auditoría oficial puede ser la ISAE 3402 (véase: http://isae3402.com/) y de certificación reconocida la ISO 27001 (véase: http://www.iso27000.es/). En el Capítulo III.c y en el Capítulo IV.b.a se ha recomendado certificaciones para la nube.

[769] Artículo 194 LCSP. La administración *"exigirá al contratista la indemnización por daños y perjuicios"*.

[770] En el subapartado b, *"Tipo contractual del cloud computing según la normativa administrativa"*, se ha concluido que en la mayoría de los supuestos nos encontraríamos dentro del contrato de servicios.

- Ante los problemas derivados del correcto funcionamiento de la infraestructura, eximiéndose de responsabilidad en los perjuicios que tengan origen en las aplicaciones o la plataforma utilizada, en la contratación *IaaS*.
- Además de las propias de los daños o perjuicios producidos por el modelo *IaaS*, será responsable por los problemas generados por la herramienta suministrada en el servicio, cuando se contrata un modelo *PaaS*. Los problemas de interoperabilidad estarían presentes en este estadio.
- Del funcionamiento de la plataforma y de las infraestructuras, cuando la Administración contrata un servicio *SaaS*.

Es primordial un ANS bien definido para evitar controversias y no se produzcan discrepancias en la interpretación del contrato, así como para garantizar que ante un cambio de proveedor se mantenga un nivel mínimo de compatibilidad de los datos registrados, posibilitando una futura migración viable, segura y rápida. Sirva para aseverar lo expuesto que la Agencia Española de Protección de Datos[771] manifiesta que los especiales requisitos de disponibilidad, confidencialidad e integridad que requieren ciertos servicios de las Administraciones públicas deben reflejarse en el contrato mediante un acuerdo de niveles de servicio, siendo necesario recoger los indicadores que determinarán la calidad del servicio y los valores mínimos aceptables.

d. Experiencias de la contratación del cloud computing en el sector público y breves notas sobre la Red SARA.

El Ayuntamiento de Barcelona, en 2013, implementó una plataforma informática en nube y utilizó el sistema *big data* para facilitar datos abiertos de la ciudad, entre otros, los procedimientos administrativos municipales y la información sobre los suministros públicos[772]. Esta apuesta por el empleo de la nube para la gestión de los datos y la información administrativa, no solo para los procesos internos, repercutirá en unos

[771] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: "Guía para clientes que contraten servicios de Cloud Computing", 2018, p. 19-23. Accesible en: https://www.aepd.es/media/guias/guia-cloud-clientes.pdf. Último acceso: 08.08.2018.

[772] MICROSOFT AZURE: "City of Barcelona - City Deploys Big Data BI Solution to Improve Lives and Create a Smart-City Template", 2013. Accesible en: https://azure.microsoft.com/es-es/case-studies/customer-stories-barcelona/. Último acceso: 08.08.2018.

"beneficios económicos acumulativos de 832 millones de euros para 2025"[773]. Muchas ciudades, bajo el influjo de un proyecto de *smart city*, han contratado servicios de *cloud computing* como herramienta facilitadora y receptora de datos e información con los distintos usuarios, internos y externos[774].

Analizado en los epígrafes anteriores el marco lógico y teórico de la contratación de la nube por las Instituciones públicas, expuestas nuestras recomendaciones para la confección de los pliegos técnicos y administrativos en la licitación del servicio y reseñando la importancia de un clausulado específico y preciso en el contrato de la nube, un estudio de casos reales de licitaciones del servicio para el sector público puede verificar las conclusiones prescritas y reforzar la consideración de que la correcta regulación de la nube, mediante los pliegos *ad hoc*, debe ser resultado de una labor multidisciplinar.

i. La nube para PATRIMONIO NACIONAL

Con el objeto de contratar el servicio de la nube, PATRIMONIO NACIONAL[775] publicó los pliegos de cláusulas administrativas y técnicas para el servicio de correo electrónico *SaaS*[776].

---

[773] WALT, Vivienne: "Barcelona: The most wired city in the world", *Fortune (web)*, 2015, publicación de 29.07.2015. Accesible en: http://fortune.com/2015/07/29/barcelona-wired-city/. Último acceso: 08.08.2018.

[774] La Agencia Española de Protección de Datos aconseja que, dada la complejidad de los servicios contratados, se designe un responsable del contrato. Esta designación, no obstante, no modifica el régimen de obligaciones y responsabilidades que debe asumir el responsable del tratamiento. Véase: "Guía para clientes que contraten servicios de Cloud Computing", 2018. Accesible en: https://www.aepd.es/media/guias/guia-cloud-clientes.pdf. Último acceso: 08.08.2018.

[775] Artículo 1 de la Ley 23/1982, de 16 de junio, reguladora del Patrimonio Nacional: *"El Consejo de Administración del Patrimonio Nacional se configura como una Entidad de Derecho público, con personalidad jurídica y capacidad de obrar, orgánicamente dependiente de la Presidencia del Gobierno…"*. Accesible en: https://www.boe.es/buscar/pdf/1982/BOE-A-1982-15230-consolidado.pdf. Último acceso: 08.08.2018. El Consejo de Administración del Patrimonio Nacional es el organismo público responsable de los bienes titularidad del Estado que proceden del legado de la Corona española, conforme a la citada Ley.

[776] El anuncio de licitación se produjo el 01.06.2015. El proceso de contratación se ha cerrado con la formalización del contrato el 05.02.2016. Se puede encontrar el expediente, junto con los documentos a los que haremos referencia, en: https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQjS_PNQvOKzc0qQpIDvY1CXNMi3Cu1HW1t9Qtycx0Bv7aTyw!!/. Último acceso: 08.08.2018.

El objeto claro y definido del contrato permite vislumbrar que realmente nos encontramos con la contratación de servicios informáticos. Dentro de las cláusulas administrativas particulares, el pliego publicita que tiene como objeto *"la prestación del servicio de correo electrónico en la nube, en modo SaaS"*, para el email corporativo de la Institución, categorizando el contrato, conforme al derogado TRLCSP, con los códigos referentes a los servicios de correo electrónico, los servicios de información con valor añadido y de proveedor de servicios de correo electrónico. La clara definición de qué necesidades pretende cubrir con el *cloud*, que posteriormente se delimitarán en las prescripciones técnicas, despeja cualquier atisbo de duda sobre el tipo contractual administrativo. Sin embargo, esta es toda regulación específica del servicio de la nube en el pliego de cláusulas administrativas particulares, el órgano de contratación estimó que toda la normativización particularizada y requerimientos de la herramienta informática se desarrollaran en el pliego de prescripciones técnicas[777].

La Entidad, en las prescripciones técnicas, comienza, de manera idéntica a la disposición recogida en el pliego de cláusulas administrativas particulares, por el requerimiento genérico de la contratación, *"servicio de correo electrónico en la nube, en modo SaaS"*, añadiendo, como actividad y servicio del adjudicatario, un acompañamiento continuo al requerir *"preparar las infraestructuras necesarias para el correo electrónico, la migración y despliegue del correo corporativo actual a la nueva plataforma"*, no solo desde un punto de vista técnico sino formativo. La Institución consideraba necesario implantar una herramienta informática que permita el acceso al correo *"desde cualquier ubicación"*. Por lo tanto, además de las características por las que se debe regir el servicio, la implantación de la nube se justifica por la adecuación entre las necesidades propias del ente contratante y la configuración del *cloud*.

En una primera aproximación, el pliego señala los condicionantes mínimos a cumplir por las propuestas presentadas por los licitadores, entre los que destacan aspectos como qué sucede con los datos y la información borrada por el usuario (*"tiempo mínimo de retención: 1 años"*), la obligación de establecer una herramienta que posibilite al contratante o los usuarios realizar exportaciones de datos e información, el respeto a los criterios recogidos por el *"Uptime Institute para la clasificación TIER III"* y la garantía

[777] Se echa de menos, como posteriormente analizaremos con el estudio de los pliegos propuestos por RED.es, que no se recojan cláusulas administrativas propias para la computación en la nube.

de una disponibilidad mínima del servicio de 99,982%. Estas características se desarrollan debidamente en cláusulas posteriores del pliego.

En los requerimientos de ejecución se manifiesta la tecnicidad del servicio y la necesidad del apoyo de los proveedores del servicio para la correcta actuación. Destacando en la cláusula de migración e implantación que se trata de un proyecto "llave en mano", exige que sea el proveedor el que realice y presente por escrito el *"plan de implantación, plan de contingencia y el plan de pruebas para la aprobación de la migración y puesta en marcha"*. A pesar de anunciarse el contenido mínimo de los documentos de las acciones anteriores, poco se instaura sobre el plan de contingencias y el plan de pruebas, esenciales al regular las incidencias, paradas y las pruebas a realizar para verificar el correcto funcionamiento de la solución informática contratada.

Hemos defendido en el presente trabajo que, ante servicios informáticos cambiantes, las cláusulas *lock-out* permiten mitigar los costes asociados a un cambio de proveedor. El presente pliego regula *"la devolución del servicio"*, con el objetivo de establecer un marco de actuación para la transferencia de conocimientos, datos y la documentación al futuro proveedor del servicio, siendo necesario el visto bueno de la Institución para dar por finalizado el contrato. Sin embargo, no delimita criterios tan importantes como el formato de transferencia, el plazo máximo de entrega al nuevo proveedor del servicio y las actividades mínimas a realizar. Idéntica consideración debe reproducirse en la cláusula de portabilidad de datos, solo exigiendo la integridad de la información y considerando el servicio incluido en el contrato, sin que pueda incurrir en costes adicionales.

El ANS, que aparece en el clausulado del documento administrativo y no en un anexo al contrato, regula de forma precisa los niveles de cumplimiento, tiempos de respuesta y tiempos de resolución del servicio, utilizando como referencia los tiempos máximos, valores objetivos y nivel de cumplimiento. Coligado a la anterior cláusula, se recogen los sistemas de penalización por incumplimiento del ANS, minuciosamente reglados. La diferente posición de las partes permite que la Institución reduzca en el abono del precio las prestaciones no realizadas o la reducción del rendimiento, con independencia de las penalidades administrativas establecidas en la normativa de aplicación. Es decir, la criticada, por nuestra parte, medida del crédito disponible por indisponibilidad o deficiencia en el servicio no tiene lugar ante sujetos que tienen un fuerte poder negociador, tanto que directamente establecen el régimen que regirá en la contratación de la nube.

Recomendamos a lo largo de la presente obra una regulación particularizada del *cloud* a través de cláusulas que recojan las características propias de la herramienta. Por ello, creemos afortunado que el pliego técnico establezca, aunque sea en un único precepto, los *"requisitos legales para los servicios de cloud computing"*. Sin embargo, el enunciado es más pretencioso que real, porque se centra exclusivamente en la ordenación de la protección de los datos y la información alojada en la nube. A pesar de la descafeinada reglamentación, sí nos parecen interesantes una serie de aspectos, que, aunque no hacen más que informar de lo establecido en la normativa de aplicación, es importante resaltar y aclarar para posicionar a las partes. De esta forma, recuerda que se requiere la formalización de la contratación de prestación de servicios con el adjudicatario, con los requisitos expuestos en el artículo 12 de la LOPD y en los artículos 20 a 22 del Reglamento de desarrollo (recordemos que la licitación se cierra antes de la vigencia del RGPD); evoca que el prestador de la nube es considerado encargado del tratamiento, actualmente regulado en la disposición adicional vigésima quinta del LCSP; y que los datos de carácter personal deben ser destruidos o devueltos a Patrimonio Nacional, o al encargado designado por la Institución, aunque nada se dice a priori de la opción establecida. Sí recoge que los datos, no lo restringe a los personales, una vez extinguido el contrato, deben borrarse a través de mecanismos que garanticen una eliminación segura. Opción que también debe ser ejecutada, en vigencia el contrato, cuando así lo solicite Patrimonio Nacional. El problema que plantea la cláusula es que será el licitador quien determine la herramienta o mecanismo de borrado, pudiendo cada licitador plantear opciones muy dispares que podrían ralentizar y obstaculizar una correcta valoración por el órgano de contratación.

Nada nuevo establece para el supuesto de la subcontratación del servicio, sin particularizar se remite a lo dispuesto en la antigua disposición adicional vigesimosexta TRLCSP, actual disposición adicional vigésima quinta LCSP, apartado 3; ni para la transferencia internacional de datos, que reproduce las recomendaciones de la AEPD[778]

[778] Para que pueda evaluarse la similitud en términos, las recomendaciones de la AEPD se encuentran en https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php . Último acceso: 08.08.2018.

conforme a la regulación establecida en los artículos 33 y 34 de la LOPD y el título IV de su reglamento de desarrollo[779].

Este somero análisis de los pliegos publicados para la contratación de un servicio *SaaS* nos muestra la complejidad de una correcta reglamentación de la nube, más ante organismos públicos que pueden no tener unas estructuras técnicas lo suficientemente desarrolladas para prever las implicaciones futuras del paso a la computación en la nube.

ii. La nube para RED.es

Cuando el órgano de contratación es un ente especializado, y puede valorar de forma reflexiva la incidencia de un cambio en la tecnología, muchas de las reseñas valoradas anteriormente son debidamente tratadas y delimitadas. Muestra de lo expuesto son los pliegos de contratación publicados por RED.es[780] para la realización del contrato de *"remedy en la nube"*[781].

El pliego de condiciones generales anticipa el contenido contractual mínimo de la nube, debidamente detallado en las condiciones particulares y en las prescripciones técnicas.

En materia de propiedad intelectual regula dos premisas necesarias, reiteradas exigencias que establecíamos en los contratos B2B: asegurar la propiedad intelectual e industrial de la información, datos, marcas y demás bienes incorporales que la Institución autoriza utilizar al prestador al amparo del contrato; y, en segundo lugar, responsabilizar al contratista del ejercicio pacífico por RED.es de todas las licencias relacionadas con la correcta implementación y utilización de la nube[782].

---

[779] En ambos casos se redacta como aportación propia del órgano de contratación, sin hacer referencia expresa a la normativa de referencia, aunque el contenido reproduce, incluso en algunos fragmentos de forma literal, lo establecido en los documentos de recomendaciones o en las disposiciones legislativas.

[780] RED.es es una entidad pública empresarial. Puedes acceder a sus Estatutos en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-3138. Último acceso: 08.08.2018.

[781] Se van a analizar los pliegos de condiciones generales, condiciones particulares y prescripciones técnicas de la contratación de referencia. Los pliegos se publicaron el 23.02.2018. Están accesibles en: https://perfilcontratante.red.es/perfilcontratante/busqueda/DetalleLicitacionesDefault.action;jsessionid=8624DDB536F172DABA2139EAF165ACFB.contratante01?idLicitacion=7005&visualizar=0. Último acceso: 08.08.2018.

[782] Se ha analizado anteriormente la incidencia del artículo 308.1 de la LCSP cuando el objeto de desarrollo del contrato lleva aparejado la puesta a disposición de productos o servicios protegidos por un derecho de propiedad intelectual o industrial, incluso cuando se excluya la cesión de derechos (subapartado b.).

Nada nuevo determina este documento en materia de protección de datos de carácter personal, instando a la aplicación de la LOPD en materia de responsabilidad sobre la utilización por el adjudicatario de los datos para una finalidad distinta a la determinada y sobre la subcontratación del servicio (licitación publicada antes de la vigencia del RGPD). Recuerda la posición del adjudicatario, encargado de tratamiento, salvo que incumpliere las estipulaciones del contrato, que sería considerado responsable del tratamiento. Sí nos ha resultado bastante oportuna la cláusula recogida cuando el proveedor almacene datos del licitador. Se señala en el pliego que *"cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales de Red.es o del adjudicatario, será preciso que exista una autorización previa de Red.es, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado"*. Aunque es una estipulación reiterada en los pliegos de la Institución, y desconociendo las verdaderas intenciones de su aparición en el documento presentado, consideramos muy conveniente su inclusión porque en la migración de datos hacia la nube el proveedor de servicios podría utilizar dispositivos físicos, garantizando, de esta forma, RED.es el control de los datos almacenados no solo en la herramienta que contrata, sino en el soporte instrumental.

Pasando a analizar el pliego de condiciones particulares, lo primero es conocer cómo se define el objeto. En la introducción del pliego se vislumbra que la voluntad del órgano de contratación es la transición de la herramienta de gestión de servicios *"Remedy AR System Server"* de una modalidad *on-premise* a *cloud computing*. Por ello, recoge que el objeto del contrato *"consiste en la prestación de un servicio de alojamiento en la nube para la herramienta Remedy AR System Server"*. Sorprende que expresamente lo defina como *"servicio de alojamiento"*, pues automáticamente nos llevaría a pensar que estamos ante una modalidad *IaaS*. Sin embargo, en las prescripciones técnicas veremos cómo se requieren unos servicios adicionales que tienden a calificar a la nube como un modelo *SaaS*.

En el subapartado "cláusulas necesarias en el contrato administrativo" del presente Capítulo considerábamos necesario combinar una característica definitoria de la nube, la posibilidad de escalabilidad, con la rigidez que frecuentemente define la redacción de los documentos administrativos. Con la delimitación de un alcance máximo, y por supuesto mínimo, la Institución permite adaptarse a las necesidades futuras de un requerimiento superior de almacenamiento o procesamiento. Así, la contratación del montante total del servicio *"está supeditada a la determinación final del uso del servicio básico… … que se*

puedan requerir derivado de las nuevas necesidades del personal o de servicios…", salvaguardando, mediante cláusula expresa, que no supone para RED.es responsabilidad alguna que, cumpliendo los supuestos establecidos, no aumente la contratación de los servicios, siempre que respete el alcance mínimo establecido en el contrato. Para la correcta valoración por el órgano de contratación, se requiere que la oferta económica desglose los servicios en precios unitarios. El pliego técnico determina cómo se establecerá la suscripción a nuevos componentes.

En el subapartado indicado también hacíamos alusión a la necesidad de considerar los derechos de propiedad intelectual, dado que los proveedores de la nube suelen incluir cláusulas, sobre todo cuando ofrecen servicios sin remuneración económica, donde se apropian de la información y los datos de la nube. RED.es directamente señala que *"adquirirá la propiedad de todo el material que sea elaborado por el adjudicatario en ejecución del contrato… en cualquier modalidad y bajo cualquier formato, para todo el mundo…"*. Añade, además, que la Institución será propietaria de todos los resultados que se realicen en cumplimiento del contrato. Obliga al adjudicatario a la entrega del código fuente y toda la documentación técnica y los entregables generados. De esta forma, la transición de un proveedor a otro se podrá realizar de forma directa e inmediata, logrando respetar los parámetros de configuración del servicio, ahora que se realiza un cambio desde *on-premise*. Ya se señaló en las condiciones generales que será el adjudicatario quien responda del ejercicio pacífico de RED.es en la utilización de la nube, con especial referencia a los derechos sobre propiedad intelectual.

Aunque podría aparecer en el pliego técnico, la Institución estima oportuno regular la subcontratación del servicio en el pliego de condiciones particulares. Para poder contratar los servicios de la nube, el adjudicatario debe incluir en la oferta la entidad subcontratista y el objeto de la subcontratación (parte de la subcontratación, porcentaje de subcontratación y perfil del subcontratista), en caso contrario requerirá la autorización de RED.es, mediante modelo formalizado. Muy oportuna es la limitación de la subcontratación en la nube, en este supuesto *"las prestaciones parciales … con terceros no podrán exceder del 60 por 100 del importe de adjudicación"*. Estos requisitos se

extrapolan a la información necesaria a aportar cuando en la licitación no se determina la posible subcontratación del servicio, requiriendo autorización expresa de la Institución[783].

Por último, antes de pasar a analizar las prescripciones técnicas, debe ponerse de manifiesto las particularidades necesarias para la seguridad de los sistemas y, con especial ahínco, para la protección de los datos. La empresa adjudicataria deberá respetar las políticas establecidas en el ENS y cumplir con las directrices ISO/IEC 27001[784]. Estando vigente el RGPD, ya hemos señalado que la ISO/IEC 27018:2014 se adecúa mejor a los requerimientos normativos exigidos. Conserva RED.es la posibilidad de auditar los planes de seguridad y los informes de auditorías del adjudicatario en los últimos seis años. Una estipulación recomendable es la concreción sobre la localización de los centros de datos, no suficientemente definida ni delimitada en el pliego por el tratamiento lacónico de la cláusula (*"en el caso de que los datos se alberguen fuera de España…"*), lo que podría restar consideración a un aspecto crucial para la correcta protección de la información contenida en la nube. Si bien, sí debemos avanzar que el pliego técnico exige que los centros de datos deberán estar localizados en la Unión Europea y, en pliego de condiciones particulares, que el adjudicatario *"deberá prestar sus servicios desde países del Espacio Económico Europeo o desde lugares que ofrezcan un nivel de protección equiparable"*, si bien, como hemos analizado, esta última cláusula no garantiza que todos los centros de datos se ubiquen donde preste los servicios de la nube el adjudicatario.

Pretendiendo no hacinar la reglamentación contenida en el pliego de prescripciones técnicas, con el objetivo de hacer ver la importancia de las diferentes cláusulas diseccionadas en los anteriores capítulos, examinaremos, en nuestra labor de exégetas, cómo pretende resolver la Institución problemas técnicos y jurídicos, aunque su disposición se encuentre diseminada a lo largo del documento.

La cláusula "requisitos de la plataforma de la nube" aventura las exigencias que aparecerán en el ANS con el contrato: se requiere un servicio con un *"volumen mínimo de 500.000 usuarios OnDemand y para al menos 1.000 entornos Remedy ITSM funcionando, con una disponibilidad media mínima de la nube de 99,9% y una*

[783] RED.es tiene la obligación de responder, por disposición contenida en el pliego, a la petición de autorización de subcontratación por el contratista. En caso contrario, transcurridos 20 días desde la solicitud, tiene la facultad de subcontratar parte del servicio.

[784] Recordemos que en el Capítulo V.a.b, dentro de la seguridad del servicio en las "cláusulas específicas en el contrato del *cloud computing*", señalábamos a la ISO/IEC 27001 como política de seguridad en los sistemas.

proactividad de detección de incidencias mínima del 98%", cláusula que se repite en diferentes estipulaciones del pliego, entre otras, en los tiempos de respuesta del servicio. Esta objetivación de los requerimientos del servicio de la nube se manifiesta en otra forma de medición. Para controlar el servicio de asesoramiento y ayuda por el proveedor, RED.es establece un calendario de soporte técnico y los objetivos de respuesta requeridos, clasificándolos en función de la severidad asociada a las incidencias, el horario de asistencia y el objetivo inicial de respuesta.

La Institución opta por tratar los niveles de servicio por separado, es decir, no recoge un documento que determine de forma específica las necesidades de funcionamiento en la nube, que, a nuestro entender, sería clarividente, puesto que a veces resulta un documento inextricable. Se limita a reconocer, como cláusula de cierre en un apartado diferenciado, que *"el adjudicatario deberá cumplir los Acuerdos de Nivel de Servicio establecidos en el presente pliego"*. Tal es el poder de negociación de RED.es que se reserva el derecho de modificar o introducir nuevos indicadores específicos, cláusula, como hemos podido comprobar a lo largo del presente trabajo, que suele reservarse el proveedor de servicios. Aunque incorpora la facultad de comprobar el cumplimiento del ANS, no señala cómo se traduce en la práctica.

En materia de protección de datos, solo como anécdota, incorpora de manera expresa el deber del adjudicatario de cumplir con el RGPD, así como con la normativa sobre Reglas Normativas Vinculantes, BCR, de la Unión Europea de aseguramiento en la transferencia de datos personales internacionales (recordemos que la licitación se publica antes de la vigencia del RGPD y otras cláusulas de los pliegos solo hacen referencia a la LOPD y al RLOPD). Más importancia tiene, por la seguridad de los datos alojados en la nube, y especialmente ante posibles ataques, robos o pérdidas de datos personales, que se recoja la obligatoriedad de ofertar un entorno aislado, es decir, no permite datos de otros clientes alojados en la nube. Intrínsecamente parece orientar el servicio a nube privada, aunque sorprende que no se defina esta exigencia en el dilatado *chek-list* de requerimientos del servicio de la nube. Una de las medidas más impactantes de las establecidas es el compromiso, por el proveedor, de que los centros de datos *Remedy OnDemand* sean abiertos, debiendo estar *"vigilados las 24 horas del día, los 365 días al año"*. Más ordinaria, señalada anteriormente, es la disposición que exige que los centros de datos estén localizados en la Unión Europea. El fin no es otro que garantizar una seguridad física y jurídica.

Qué duda cabe que para el sector público es esencial, como acopiáramos *ad supra* al estudiar las consideraciones del Grupo de Trabajo del artículo 29, que terminado el servicio con el proveedor se destruyan los datos alojados en la nube del proveedor de manera segura. La destrucción física del *hardware* se descarta por los costes asociados y la posible imposibilidad técnica, deslocalización. Una alternativa razonable recoge el pliego de condiciones, *"destruidos a través de la eliminación de las claves de encriptación de base de datos"* y, para los datos de carácter no personal, sobreescribirlos con ceros binarios. No solo regula la eliminación cuando se termina el servicio, sino que establece la retención de los archivos de datos *backup* en función del entorno, la frecuencia y la ubicación del almacenamiento.

El cambio de proveedor de la nube genera costes e incompatibilidad del servicio. Deviene necesario, por tanto, la regulación de la extracción de los datos alojados en la nube. Para ello, RED.es exige el servicio de extracción de datos *"en un archivo que contenga todos los datos en un formato de valores separados por comas"* (.csv, documento en formato abierto) o *"un formato de backup de base de datos a pedidos"*. Además, dentro de la devolución del servicio, se faculta a la Institución, sin que suponga un sobrecoste, exigir al adjudicatario la transferencia del conocimiento actualizada del proyecto a la entidad que RED.es determine, con una antelación mínima de 30 días laborables antes de la finalización del contrato. Se complementa, la medida, con la obligatoriedad de, por parte del proveedor de servicios, presentar un modelo de nube que permita la integración de datos *"hacia y desde sus servicios OnDemand"*, estableciendo el método o adaptador aprobado.

Incorporar en el contrato la monitorización del servicio para su correcta ejecución ha sido una de las medidas defendidas en este trabajo para posibilitar al contratante medios de pruebas continuos. Sin embargo, RED.es amplía estas posibilidades de monitorización a los centros de datos, en particular a los sistemas eléctricos, ambientales y de *backup*. El problema es que no define si esta monitorización es obligación del prestador del servicio, sin que la Institución tenga el derecho a acceder a los medios necesarios para confirmar la actividad, o, lo que sería más garantista, si RED.es tendría la facultad de acceder a los medios de vigilancia y monitoreos indicados. Parece que se tiende a esta segunda posibilidad al reconocer que *"proporcionará acceso a una página de estado en modalidad autoservicio. Esta página de estado ofrecerá una herramienta en tiempo real para supervisar la actividad y el uso de la misma"*. Es, sin embargo, una interpretación

extensiva, pues el desarrollo de este monitoreo se centra en el *"Remedy OnDemand",* sin especificar la inclusión de los centros de datos. En la cláusula específica sobre la monitorización, delimita que todos los servicios serán monitorizados *"24x7"* con un nivel de incidencias mínimas del 98%.

Para finalizar, queremos destacar la conveniencia de la cláusula que delimita quién es responsable del correcto desarrollo del servicio en función de quién controla el proceso formal de gestión de cambios. En un servicio informático donde la pericia humana en la correcta gestión de la herramienta y los procesos técnicos están interconectados con difícil disgregación, este precepto, en una primera aproximación y sin perjuicio de un posterior análisis pormenorizado, categoriza en función de la actividad (que incluye no solo la etiqueta sino la definición de esta y una serie de notas) la parte responsable de garantizar el correcto funcionamiento del servicio.

Los pliegos analizados demuestran que las Instituciones y organizaciones del sector público, cumpliendo con el régimen jurídico específico aplicable a estos entes, pueden reglamentar la contratación de la nube en una posición privilegiada comparada con los consumidores y pequeñas o medianas empresas o profesionales. Las advertencias y recomendaciones examinadas a lo largo del presente trabajo se ponen de manifiesto y se materializan en los pliegos que regulan la contratación de la nube, sobre todo ante organismos especializados, es decir, hay un proceso de análisis de las incidencias que podría tener la implantación del *cloud* en la Institución. Sin embargo, se ha observado que este análisis profundo técnico desvirtúa la claridad que es recomendable en la presentación de una licitación de carácter administrativo. No presentar un modelo armonizado, donde diferentes cláusulas, dispersas por el documento administrativo, regulan aspectos conexos, dificulta la comprensión. De igual forma, se ha puesto de manifiesto que, dependiendo del órgano contratante, el proceso de tratamiento y estudio de la nube tiene un mayor o menor grado de profundidad. Por ello, se cree oportuno erigir un equipo responsable de analizar y consolidar, de forma circunspecta, los problemas técnicos que plantea la herramienta con las consecuencias jurídicas de la implantación de la nube, vindicando documentos técnicos-administrativos que recojan las particularidades de los entes públicos.

iii. La red SARA para las Administraciones públicas en España

Para finalizar este opúsculo sobre la contratación de la nube en el sector público, unas breves notas sobre la red SARA como plataforma de servicios en la nube para las Administraciones públicas, a modo de excurso, nos adentrará en la estrategia estatal sobre la implantación de la herramienta informática.

El Consejo Superior de Administración Electrónica, el 15 de enero de 2013, señaló que la Red SARA es un proyecto prioritario para que todas las administraciones compartan los servicios en la nube, proyecto para comenzar a construir una red privada en las Administraciones públicas españolas que conduzca a un ahorro en costes e inversión, reduciendo la brecha digital[785]. Como señala el OBSAE[786], la construcción de infraestructuras propias para la creación de una nube privada para la administración es compatible con cualquier solución de *cloud* público.

La red SARA surge como instrumento fausto de desarrollo de la administración electrónica, al amparo de la LAE y del ENI, a través de la cual cualquier organismo público puede, tras incorporarse a la red de forma gratuita y bajo convenio, obtener, implementar y utilizar diferentes servicios como la verificación de los datos de identidad y residencia, la plataforma de validación de firma electrónica (@Firma), y el registro electrónico común o la mensajería instantánea, entre otros[787]. En general, la Administración estatal provee una herramienta que pretende agrupar las infraestructuras tecnológicas para conectar a todas las administraciones y facilitar un intercambio de

[785] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS – CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA: "Aprobadas las líneas estratégicas del plan de Administración Electrónica del Gobierno 2013-2015", 2013, nota de prensa del 15.01.2013. Accesible en: http://www.minhafp.gob.es/Documentacion/Publico/GabineteMinistro/Notas%20Prensa/2013/S.E.%20ADMINISTRACIONES%20PUBLICAS/15-01-13%20NP%20CS%20Administraci%C3%B3n%20Electr%C3%B3nica.pdf. Último acceso: 08.08.2018.

[786] OBSAE: "Hacia una estrategia de Cloud Computing en las Administraciones Públicas", 2013, p. 2. Accesible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:99490b88-c2d4-4ca1-b16e-140fa7caf13c/2013-02_nota_tecnica_CLOUD.pdf. Último acceso: 08.08.2018.

[787] Todos los servicios se encuentran en la web oficial, Portal de Administración Electrónica: https://administracionelectronica.gob.es/ctt/redsara/infoadicional#.Wth3PIjFI2w. Último acceso: 08.08.2018.

aplicaciones, información y servicios, propiciando un sistema de intercambio de conexiones en condiciones óptimas[788].

Las características técnicas principales de la Red SARA[789] permiten la adopción de la nube. La capacidad de la red, principalmente por los centros de datos suministrados por los proveedores del servicio que permiten asegurar la demanda de la administración electrónica; el punto-multipunto, sin un nodo central, que se ve reforzado por la configuración de la nube a través de diferentes centros de datos y con una conexión multipunto, con cualquier ancho de banda contratado por las Administraciones; y la flexibilidad de la computación en la nube, propicia la elasticidad y rapidez en la provisión del servicio requerida por los entes públicos.

La computación en la nube, por tanto, aparece como la herramienta informática actual para la coordinación de datos e información entre Administraciones. A día de hoy, son 4.000 entidades locales (acumulado) conectadas a la Red SARA[790].

[788] Aunque no es una publicación reciente, la Guía de la Red SARA "La Administración de mañana, hoy", permite al lector estructurar y aclarar los servicios y las jerarquías establecidas en la herramienta. La arquitectura técnica sí ha sufrido modificaciones. FABEIRO SANZ, Jorge: "Guía de la Red Sara. La Administración de mañana, hoy", *Dirección General para el impulso de la Administración Electrónica,* 2008.

[789] Para ver las características técnicas principales, independientemente de la herramienta informática utilizada: DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA: "Guía de aplicación de la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las AA.PP. españolas", *Ministerio de Política Territorial y Administración Pública. Secretaría General Técnica*, 2011, p.14. Accesible en: http://www.sefp.minhafp.gob.es/dam/es/web/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_conex-red-AA-PP-esp-INTERNET.pdf. Último acceso: 08.08.2018.

[790] 20.04.2018. Dato extraído del Portal de Administración Electrónica. Accesible en: https://administracionelectronica.gob.es/ctt/redsara/mas#.WtnQ14jFLIV. Último acceso: 20.04.2018.

CONCLUSIONES

Como corolario al presente trabajo, exponemos las principales conclusiones de la disertación sobre la contratación de la computación en la nube a modo de epítome.

I. Independientemente del modelo de servicio y la forma de implantación de la nube, sin perjuicio de una regulación propia del servicio por sus características singulares, nada impide la aplicación del Derecho de contratos. Con una actitud circunspecta, los problemas jurídicos que se presentan en la ejecución del objeto del contrato pueden ser estudiados, a falta de un desarrollo normativo, por las disposiciones vigentes en el ordenamiento jurídico. Las ventajas competitivas que supone la implantación de la nube para empresas, consumidores e Instituciones públicas resultan obvias, principalmente por el ahorro en costes y la mejora en la eficiencia productiva.

II. Por la información que los clientes incorporan a la nube, que puede afectar a la viabilidad del negocio, a las obligaciones impuestas para con los administrados o a datos de carácter personal, entre otros, deviene necesario establecer el marco jurídico que debe amparar en la contratación de la herramienta informática, que a menudo se encuentra con condiciones generales impuestas por los proveedores, amparados en un clausulado lóbrego. Los términos preestablecidos por los proveedores del servicio reflejan un modelo de distribución de consumo.

III. No existe un concepto generalizado del *cloud computing*, esta tecnología ha sido definida por los modelos de servicios ofrecidos actualmente por los proveedores. Este hecho podría dificultar la regulación presente y futura de la nube, contraviniendo el principio de neutralidad tecnológica. Por este motivo, hemos defendido la utilización de un concepto tecnológicamente neutro, impulsado por las características esenciales del servicio.

IV. Las características esenciales de la herramienta informática no solo definirán el servicio, sino que determinarán los problemas jurídicos a los que dar respuesta. Se erige necesario, por tanto, tener presente que nos encontramos ante un servicio bajo demanda, donde la interacción interpersonal es mínima; que es una herramienta que necesita del acceso a la red, pretende una disposición de datos y aplicaciones en cualquier lugar y desde cualquier dispositivo; se constituye como un servicio a disposición de múltiples clientes;

la provisión del servicio se caracteriza por la elasticidad y la rapidez, eliminando la posibilidad de medios infrautilizados; y se configura como un servicio mensurable. Sumado a la desmaterialización de la herramienta informática, la distribución de la nube en tres capas y la posibilidad de establecer un pago del servicio por consumo real, permiten diferenciar al *cloud* de otros servicios informáticos.

V. Las características de la nube determinan los potenciales riesgos a asumir ante su implantación. La seguridad de los datos trasladados a la nube, la privacidad y confidencialidad de la información y los datos, la autentificación de los usuarios, la disponibilidad del servicio, la propiedad de los contenidos, los problemas relacionados con la propiedad intelectual e industrial de las herramientas utilizadas y de los datos y la información generada, y la interconexión entre diferentes sistemas, deben ser analizados y valorados por los clientes, en función de las necesidades y su modelo de negocio, antes de adoptar el *cloud*. Los clientes no somos omniscientes, requeriremos en las distintas fases del proceso de contratación colaboración y ayuda externa.

VI. El carácter internacional del servicio, la deslocalización en el almacenamiento de datos y la falta de una gobernanza internacional, unido a la posición dominante de las empresas del sector, han favorecido a la implantación generalizada de cláusulas de adhesión y predispuestas como instrumento regulador de la relación comercial.

VII. Los contratos informáticos, categoría aplicable a la computación en la nube por razón de su objeto, y los contratos electrónicos, medio habitual por el que se conforma y se perfecciona la voluntad de las partes en el *cloud*, tenemos que encuadrarlos en la teoría general de contratos. La atipicidad del contrato de la computación en la nube, que mezcla obligaciones de medios y resultados, no es óbice para acudir a los estándares y principios internacionales del comercio electrónico como respuesta a las nuevas relaciones de negocios, solucionando las posibles contradicciones o lagunas del ordenamiento jurídico.

VIII. El principio de buena fe sobre la base de las relaciones entre partes y el principio de autonomía de la voluntad, donde las partes dotan de contenido la relación contractual, se instituyen como principios esenciales y vertebradores de la contratación electrónica. Sin embargo, la completa compatibilidad y

equivalencia entre los soportes tradicionales y los medios electrónicos requieren la aplicación de principios consolidados en la esfera internacional del comercio electrónico: el principio de libertad de forma, que propicia que las partes queden obligadas en cualquiera de la forma que determinen los sujetos intervinientes; el principio de inalterabilidad del Derecho preexistente, que propugna que el medio no condiciona un nuevo marco regulador; el principio de no discriminación, por el cual el régimen jurídico de los contratos no es modificado por razón del medio empleado; el principio de equivalencia funcional, que permite aplicar los mismos efectos jurídicos a los medios electrónicos que a los tradicionales, sin modificar el Derecho sustantivo; y el principio de neutralidad normativa en relación con la tecnología, para no condicionar el empleo de unos medios frente a otros, son principios universales presentes en la contratación de la nube.

IX. Los textos e iniciativas que se han aproximado a la realidad del *cloud* o han intentado regular la incidencia de la nube, en el marco internacional o en un estado embrionario en nuestro ordenamiento jurídico, pretenden dar respuesta, principalmente, a la intervención de dos conjuntos de contratantes: los entes que componen el sector público y los profesionales y empresas, es decir, las relaciones B2A y B2B. Las perspectivas y objetivos han marcado la extensibilidad de los trabajos para una respuesta a la nueva realidad de la nube. En el marco internacional, los documentos han centrado su análisis, estudio y regulación en las relaciones B2A. Con diferente profundidad, y consolidando una forma de dar respuesta a la contratación de la nube y el empleo de un lenguaje que de forma uniforme se impone en el sector, la seguridad del servicio, en sus diferentes vertientes, es la razón manifiesta de las iniciativas. Tematizados, por su propia razón de ser, los documentos elaborados por el Grupo de Trabajo del artículo 29 han dado luz a una nueva realidad, donde definir y delimitar la responsabilidad y obligaciones de los sujetos que intervienen en el tratamiento de datos personales en la nube, ha supuesto un reto por la deslocalización, la cadena de sujetos intervinientes en el proceso y, en general, por lo novedoso de la herramienta informática. Los trabajos han sido el germen de la posterior regulación, que tiene como principal valedor el RGPD. Este proceso de análisis y estudio ha reforzado los preceptos que

contuviera la Directiva 95/46/CE, laxos y no definitorios ante la evolución de nuevas herramientas informáticas.

X. El Anteproyecto de Ley de Código Mercantil español, aunque en la tipificación de los contratos de comunicaciones electrónicas no se recoja la realidad del *cloud computing*, sí permite vislumbrar las principales obligaciones de los sujetos intervinientes de la relación comercial, así como las responsabilidades en caso de incumplimiento. Depende del modelo de implantación en la nube y la configuración al usuario, la aplicación de los supuestos tipificados puede ser analógica.

XI. El Grupo de Trabajo IV de la CNUDMI es el primer organismo de carácter internacional que de forma holística conforma una guía jurídica sobre la computación en la nube, reconociendo la idiosincrasia del servicio. Aunque de carácter propositivo, puede ser el punto de partida para que los Estados configuren el tratamiento de esta nueva realidad y, para los clientes, supone una guía sobre los riesgos y consecuencias del empleo del servicio informático.

XII. La protección de datos de carácter personal es una temática recurrente en el empleo de las herramientas informáticas, más cuando, como la nube, la deslocalización de los servidores dificulta la aplicación de la normativa a efecto. La labor de la doctrina y del Grupo del Trabajo del artículo 29 han permitido definir la posición jurídica del proveedor de la nube, encargado del tratamiento, y del cliente, responsable del tratamiento, siempre que este último ostente la capacidad para determinar la finalidad, contenido y uso del tratamiento de datos. Reside en el cliente la obligación de actuar con suma cautela en la elección del proveedor, no solo por la necesaria colaboración de ambos sujetos en el correcto desarrollo del servicio y de las obligaciones que les impone el RGPD, sino porque recae bajo la responsabilidad del cliente la mala actuación del encargado. El RGPD ha reforzado las prerrogativas del interesado, teniendo la potestad de conocer las condiciones en las que se realiza el tratamiento de datos y ampliando sus derechos, como el conocido de portabilidad y el derecho al olvido.

XIII. El contrato entre el cliente, no necesariamente coincidente con el interesado de los datos, y el encargado del tratamiento de datos personales, debe ser analizado con sumo detalle. El acceso de datos por el prestador de la nube

exige un deber de colaboración, transparencia y diligencia entre partes, necesariamente provisto de un contrato u otro acto jurídico con arreglo a Derecho. Con un contenido mínimo, ampliado tras la vigencia del RGPD, supone la plasmación de la finalidad, duración y naturaleza del tratamiento, el tipo de datos personales y la categoría de interesados, las obligaciones y derechos del responsable de datos, la exigencia de confidencialidad en el tratamiento, la correcta asistencia del encargado, la supresión o devolución de los datos terminado el encargo y la puesta a disposición del cliente de los medios probatorios que garanticen la correcta aplicación de la normativa, entre otros. Este contenido, que se hace extensible a las subcontrataciones del servicio, propicia la transparencia, se reconoce el principio de *accountability*, y el conocimiento efectivo por los clientes de la nube y los interesados, de vital importancia tras las obligaciones y sanciones impuestas por el RGPD. Habrá que esperar a la definitiva elaboración de la norma nacional de protección de datos para determinar el alcance y concreción en aquellos aspectos que el RGPD posibilita regular a los Estados.

XIV. Por la naturaleza de la nube, en materia de protección de datos personales, la subcontratación del servicio y las transferencias internacionales de datos son problemas recurrentes. La manifestación expresa de la posibilidad de subcontratación en el RGPD, bajo el paraguas del contrato con instrucciones documentadas, siendo necesaria la autorización previa por escrito del responsable, y la asimilación del subencargado de las mismas obligaciones contenidas en el contrato originario, refuerzan las garantías para una correcta adecuación a la normativa. En materia de transferencias internacionales de datos, el RGPD, a nuestro juicio, ha esclarecido los instrumentos que ofrecen garantías adecuadas para efectuarlas a terceros países, determinando de manera clara aquellos que requieren autorización de la autoridad de control y regulando, necesario por la práctica de la gestión del negocio, las NCV. Sí es necesario una actualización, a nuestro parecer, de las cláusulas tipo para la transferencia internacional de datos, así como regular un supuesto de hecho que, hasta la fecha, no ha sido configurado: la subcontratación entre un encargado establecido en un Estado Miembro o del EEE y un subencargado establecido en un tercer país.

XV. El contrato, por tanto, se erige como el instrumento jurídico propicio para regular el paradigma de la nube, con el fin de determinar el alcance de la nube, los niveles de servicio y la disponibilidad a satisfacer por los proveedores, las localizaciones de los datos en la nube, las obligaciones en materia de seguridad y de protección de datos, la responsabilidad del proveedor de la nube y las obligaciones y derechos de las partes extinto o resuelto el contrato de *cloud*. En la fase precontractual, el cliente previsiblemente requerirá un asesoramiento externo y previo, debido a la desigualdad de las partes y a la tecnicidad del servicio. Determinar la finalidad pretendida debe ser el objetivo de esta primera fase. En la perfección del contrato, debe declararse de manera clara y concisa el objeto y las fases del desarrollo del producto. Y en la etapa de desarrollo y ejecución, será esencial determinar las responsabilidades de las partes en caso de incumplimiento.

XVI. La nube es un servicio bajo demanda, que requiere elasticidad y rapidez en su provisión, mensurable, siendo necesario convenir las condiciones de continuidad, regularidad, velocidad, volumen y seguridad. Las obligaciones del proveedor del servicio, por tanto, estarán relacionadas con garantizar la prestación del servicio, la disponibilidad o acceso ininterrumpido, la integridad y la confidencialidad de datos. Será necesario, además, la colaboración con el cliente, dado que este requerirá información sobre la nube para adecuarla a sus necesidades. Como relación sinalagmática, el cliente se obliga, principalmente, al pago del precio por los servicios aplicados, al cumplimiento de las políticas de uso de la nube y a colaborar con el proveedor del servicio.

XVII. El ANS se configura, junto con la AUP, que tienden a un inextricable contenido, como los anexos principales del contrato en la nube. La importancia de una correcta evaluación del ANS se manifiesta en las tres fases de la vida de la nube: permite al cliente valorar las opciones del mercado según sus necesidades, determina si se cumplen los niveles de servicio definidos y permite practicar medidas correctivas, y su valoración final determinará la correcta ejecución del servicio y permitirá ejercer acciones ante sus incumplimientos. Aunque la naturaleza del servicio propicie que el proveedor actualice su ANS en vigencia del contrato, es oportuno que el proveedor proporcione información de los cambios, que no requieran una sobre carga al

cliente, y, en última instancia, se faculte al cliente de rescindir el contrato sin penalización si no se adecúa a sus necesidades actuales.

XVIII. Los proveedores de la nube suelen limitar la responsabilidad ante un cumplimiento defectuoso, reconociendo, cuando así lo hacen, solo las pérdidas directas y los recursos económicos pagados, a través de créditos en el servicio. El deber de diligencia del prestador del servicio será determinante para orientar los límites a la responsabilidad en las relaciones B2B. A falta de regulación en el contrato, nuestro ordenamiento jurídico reconoce la responsabilidad contractual del proveedor en los artículos 1.101 y ss. del CC, si bien, cuando los defectos en la prestación devienen de la actuación de los subproveedores, habrá que atenerse al régimen de la responsabilidad extracontractual, 1.902 y ss del CC, sin perjuicio de que el proveedor principal repita los importes satisfechos. Sin embargo, no debe obviarse que deberá valorarse la actuación de las partes eligiendo a los subproveedores del servicio, sobre todo el conocimiento del cliente y sus facultades de veto.

XIX. Las causas de extinción del contrato del *cloud* y el efecto de las obligaciones no son debidamente estudiados en la contratación del servicio, y no suelen estar suficientemente regulados en el documento contractual. Qué sucederá con los datos y la información en la nube y las obligaciones del proveedor, principalmente las relacionadas con la reversibilidad del servicio, deben ser *ítems* esenciales en la evaluación del correcto proveedor. Es común restringir las posibilidades, sin penalización, de un desistimiento unilateral del contratante y, sobre todo, repercutir en el cliente las consecuencias de una imposibilidad sobrevenida en la prestación del servicio, siendo habituales cargas adicionales.

XX. En pos de la transparencia y la confianza de los clientes en la adopción del servicio, es conveniente establecer procedimientos internos con el proveedor ante supuestos que den lugar a la suspensión del servicio. Sobre la base de solventar o subsanar los problemas acaecidos y evitar la resolución, reequilibra el poder de las partes del contrato. Ante la imposibilidad de resolver las incidencias o terminado el contrato por cualquier otra causa, es oportuno que el proveedor se obligue al borrado de los datos trasladados al servicio, recordemos que en el *cloud* el proveedor debe guardar

confidencialidad, pero no está obligado al borrado de los datos, salvo que estos tuvieran carácter de personales.

XXI. El desequilibrio manifiesto en la contratación de la nube entre empresarios pretende ser contrarrestado cuando el contratante es un consumidor, a través de normas tuitivas. El empleo de los medios electrónicos, con conexiones con ordenamientos jurídicos internacionales, y la configuración de la herramienta, que propicia un uso mixto y la contratación con proveedores con un sistema jurídico distinto al del cliente, requiere que de forma clarividente se determine quién es el sujeto objetivo de protección y el ámbito de aplicación de las normas a la luz del Derecho Internacional Privado. En otro orden, aunque las cláusulas de la nube tienen, en general, carácter de predispuestas, se incorporan de manera unilateral por parte del proveedor, se dirigen a una pluralidad de clientes y se incorporan al contrato, por lo tanto, sería de aplicación la LCGC y el TRLCU, debemos cerciorarnos de que no nos encontramos en un supuesto de adhesión particular. En este marco protector, los criterios de cognoscibilidad y comprensibilidad de las cláusulas en las condiciones generales deben desplegar todos sus efectos jurídicos, que corresponderán combinarse con la obligación de información de carácter previo que impone la LSSICE al prestador del servicio.

XXII. La protección al consumidor de la nube se conmina en dos momentos: antes de la contratación, cuya finalidad es que el cliente obtenga la información necesaria antes de la celebración del contrato para que pueda prestar un consentimiento informado; y una protección *ex post*, para reparar el desequilibrio producido por la incorporación de cláusulas abusivas o poco transparentes. El núcleo de la defensa al consumidor se centra en este segundo momento, creemos que por dos cuestiones principalmente. En primer lugar, cada vez son más los clientes que deciden aventurarse en la búsqueda y contratación del servicio con proveedores radicados en terceros países. Internet pone al alcance de los usuarios un mercado global, posibilitando la contratación con prestadores que no dirigen su oferta, sectorialmente, al mercado español. En segundo lugar, porque el empleo de la nube en muchos supuestos es de carácter "obligatorio", para una funcionalidad total de los dispositivos. Por estos motivos, entre otros, y aunque defendamos que es esencial que el cliente sea consciente de los pros y contras de la contratación

y de un conocimiento exacto de los derechos y obligaciones que supone la adopción del servicio, lo que requiere una valoración *ex ante* para un consentimiento informado, entendemos que las normas reguladoras se centren en el control de las cláusulas incorporadas al contrato.

XXIII. Esta protección en las condiciones generales de la contratación y en las cláusulas específicas del contrato del *cloud*, nos hace reflexionar cómo sujetos que en principio se encontraría en una situación similar respecto al poder de negociación, autónomo y consumidor, tienen una protección radicalmente distinta. La consideración de no puestas, en palabras del Tribunal Supremo, de las cláusulas abusivas para los consumidores, que pueden incidir en la reglamentación de aspectos tan importantes como la protección de los datos, la variación de los términos del contrato o del ANS, la responsabilidad o la asunción de un foro y ley aplicable, por citar solo algunos ejemplos, permiten un marco de garantía para la parte más débil del contrato que no encuentra, como decimos, el pequeño empresario, profesional o PYME.

XXIV. La LCGC es de aplicación a los contratos de adhesión, ante condiciones generales predispuestas, incluyendo a contratantes consumidores y no consumidores. Esta condición de parte débil en el contrato, que propicia un claro desequilibrio entre predisponente y adherente, sin libertad negocial, justifica someter las cláusulas a un control de incorporación. Como se dejó de manifiesto en nuestro estudio, la finalidad es que el pequeño empresario, en este caso, conozca de la existencia y el alcance de las cláusulas, para lo cual requieren que estas sean transparentes. El control del contenido, cuando el contratante es un empresario o profesional, estará determinado por la no contravención a las disposiciones generales en materia de contratos, es decir, sean conformes a las leyes, la moral o el orden público. Por otra parte, el CC aduce que la interpretación de cláusulas oscuras favorecerá a la parte que no hubiere ocasionado la oscuridad. Por lo tanto, la protección al pequeño empresario o profesional dependerá principalmente de su poder de negociación, su capacidad económica, los conocimientos en la materia y la necesidad de adquirir el servicio de *cloud*. Con estas premisas, habrá que valorar la nulidad de las cláusulas conforme a la LCGC, teniendo presente que el CC establece los principios de buena fe y equilibrio contractual, preceptúa

una interpretación favorable al adherente ante cláusulas oscuras y requiere que las cláusulas no vulneren la moral, el orden público ni las leyes existentes.

XXV. La estrategia sobre la implementación de la administración electrónica aparece con la erupción de las primeras herramientas informáticas colaborativas, con el objetivo, a nuestro entender pretensioso por no contar con los medios adecuados, de transformar, de forma transversal, los métodos de trabajo, la interrelación entre administraciones y la comunicación con los administrados. Esta visión expansiva y extensiva de la administración electrónica puede ser efectiva con el empleo de la nube. El marco normativo actual, principalmente la LPACAP y LRJSP, impele el empleo de herramientas electrónicas de "papel cero" e intentan aliviar la carga de los administrados en el acceso, consulta y aportación de documentos administrativos. Mas, las dificultades podrían presentarse con el tipo contractual de la nube según el marco regulador administrativo. Aunque habrá que atender a la correcta configurar del *cloud*, el régimen jurídico establecido para los contratos de servicios se configura como el marco jurídico aplicable a la contratación de la nube por las Administraciones públicas.

XXVI. Las incidencias que pueden aparecer con la adopción del servicio, y que deben ser resultas en las cláusulas publicadas en los expedientes administrativos y técnicos de la licitación, no difieren, en gran medida, de las que se enfrentan las empresas y los consumidores, si bien, deben atender a la regulación sustantiva. Por la naturaleza de los datos y la información a tratar deberá analizarse con ahínco la autenticidad, integridad, disponibilidad, trazabilidad, calidad, protección, recuperación, conservación física y logística de los sistemas electrónicos, así como los métodos de borrado, eliminación y destrucción durante la ejecución y finalizado el contrato, siempre bajo el paraguas regulador del ENS y el ENI. Sí puede observarse una gran diferencia entre sujetos contratantes cuando uno es una Administración pública, el poder negociador y su capacidad para imponer una reglamentación, principalmente por su capacidad de acudir a un mercado no estandarizado sino de servicios elaborados *ad hoc*. Si bien, al igual que en otros supuestos, las pequeñas Instituciones se encontrarán con restricciones. Por este motivo es recomendable la adopción de Acuerdos Marco implantados en el contexto internacional, principalmente el G-Cloud UK, al recoger los estándares

mínimos necesarios para la contratación pública. Este tipo de acuerdos, permiten agilizar el proceso de contratación, favoreciendo no solo a las Instituciones sino al entorno empresarial y a los usuarios, al determinarse unos criterios técnicos mínimos y al procederse a evaluar, sobre la base de esos criterios, las distintas ofertas del mercado de la nube.

XXVII. Los riesgos jurídicos expuestos no deben desalentar la implantación de los servicios de *cloud* por los distintos clientes. No tendemos a la distopía, más al contrario, se incide en ellos para adecuar de manera efectiva las necesidades de los clientes con los estándares del servicio, vindicando una gestión responsable de la computación en la nube. Sí sería oportuno reflexionar sobre la necesidad de extender una protección jurídica, al alimón de las reglas tuitivas para consumidores, de los pequeños empresarios o profesionales que no tienen capacidad de negociación y se encuentran con cláusulas predispuestas que pueden mermar su protección, en sentido amplio, al adoptar esta nueva tecnología, muchas veces impuestas por el desarrollo de las TIC.

BIBLIOGRAFÍA Y DOCUMENTACIÓN[791]

A

ACÍN FERRER, Ángela: "Procedimiento administrativo. Administración electrónica. Derecho de acceso a la información. La difícil aplicación de la Ley del Procedimiento Administrativo Común", *La Administración Práctica*, 2015, Cizur Menor, núm. 6/2015, parte comentario.

ADICAE: "Análisis de la contratación y compra a distancia y sus principales problemas para los consumidores", *Proyecto: Consumidores 2014. Retos y mejoras en sus derechos a la hora de contratar y en su defensa colectiva*, 2014. Accesible en: http://blog.adicae.net/consumidores-2014/files/2014/12/InformeADICAEFinalFinal.pdf. Último acceso: 08.08.2018.

ADJUDICACIONES Y LICITACIONES TIC: "Barómetro Inversión del Sector Público – Informe Semestral", 2017, 1er Semestre. Accesible en: http://www.adjudicacionestic.com/front/articulo-contenido.php?id=129 (bajo registro). Último acceso: 08.08.2018.

AEPD: "Guía para clientes que contraten servicios de Cloud Computing", 2018. Accesible en: https://www.aepd.es/media/guias/guia-cloud-clientes.pdf. Último acceso: 08.08.2018.

AEPD: "Orientaciones para prestadores de servicios de Cloud Computing", 2018. Accesible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf. Último acceso: 08.08.2018.

AEPD: "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento", 2017. Accesible en: https://www.aepd.es/media/guias/guia-directrices-contratos.pdf. Último acceso: 08.08.2018.

AEPD: "El Delegado de Protección de Datos en las Administraciones Públicas", 2017. Accesible en: https://www.aepd.es/media/docs/funciones-dpd-en-aapp.pdf. Último acceso: 08.08.2018.

AEPD: "Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento", 2017. Accesible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf. Último acceso: 08.08.2018

AEPD: "Informe 0157/2012", 2012.

AEPD: "Resolución del expediente número TI/00126/2012", 2012.

[791] La clasificación es por orden alfabético del autor del documento o de la Institución que lo publica. En segundo lugar, ante varias obras del mismo autor o publicaciones de una misma Institución, se primará la fecha de publicación.

AEPD: “Contribución de la Agencia Española de Protección de Datos a la consulta de la comisión sobre un enfoque global de la protección de datos personales en la Unión Europea”, 2011.

AEPD: “Recomendaciones referentes al Plan de Inspección de Oficio a las empresas participantes en la elaboración de los Censos de Población y Viviendas del año 2001”, 2003 (17.07.2003).

ALARCÓN FIDALGO, Joaquín: “Cloud computing, responsabilidad y seguro”, *Revista Española de Seguros*, 2013, nº 153-154.

ALERTLOGIC: “Cloud security report. Research on the Evolving State of Cloud Security”, 2017. Accesible en (bajo petición): https://www.alertlogic.com/resources/cloud-security-report-2017. Último acceso: 08.08.2018.

ALI, Mazhar; KHAN, Samee U.; y VASILAKOS, Athanasios V.: “Security in cloud computing: Opportunities and challenges”, *Information Sciences*, 2015.

ÁLVAREZ DE SOTOMAYOR, Silvia Feliu: “Nulidad de las cláusulas de jurisdicción y ley aplicable a la luz de la Ley 3/2014 por la que se modifica el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios”, *Revista electrónica de estudios internacionales (REEI)*, 2015, nº 29. Accesible en: http://www.reei.org/index.php/revista/num29/archivos/Estudio_FELIU_Silvia.pdf. Último acceso: 08.08.2018.

ÁLVAREZ HERNANDO, Javier: “El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades”, *Manual de las principales novedades del Reglamento Europeo de Protección de Datos*, 2018, Thomson Reuters.

ÁLVAREZ MORENO, María Teresa: “Ámbito de aplicación subjetivo”, *Protección jurídica del consumidor en la contratación en general: normas imperativas y pactos al respecto*, 2015, Reus.

ÁLVAREZ RIGAUDIAS, Cecilia: “Condiciones para las transferencias internacionales de datos personales en servicios de cloud”. *Derecho y cloud computing*, 2012.

ANDERSON, Cushing y GANTZ, John F.: “Climate Change: Cloud´s Impacto on IT Organizations and Stafflin*”, Microsoft White Paper*, 2012. Accesible en: https://news.microsoft.com/download/presskits/learning/docs/IDC.pdf. Último acceso: 08.08.2018.

APARICIO VAQUERO, Juan Pablo: “Contratación informática y outsourcing”, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 2002, Comares.

APARICIO VAQUERO, Juan Pablo: "Elementos y naturaleza de la relación de outsourcing", *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 2002, Comares.

ARTICLE 29 DATA PROTECTION WORKING PARTY: "Opinion 5/2012 on cloud computing, 2012, 01037/12/EN WP 196 (01.07.2012)", 2012. Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Último acceso: 08.08.2018.

ASENSI MERÁS, Altea: "Los contratos para las comunicaciones electrónicas", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, 2015, Universidad Carlos III de Madrid.

B

BAR-MAGEN, Jonathan: "Fog computing. Introduction to a New Cloud Evolution", *Escrituras silenciadas: paisaje como historiografía*, 2013.

BARRIUSO RUIZ, Carlos: "La formación del contrato electrónico", *La contratación electrónica*, 2002, Dykinson.

BATISTA DE CARVALHO, Carlos André; DE CASTRO ANDRADE, Rossana Maria; FRANKLIN DE CASTRO, Miguel; FERREIRA COUTINHO, Emanuel; y AGOULMINE, Nazim: "State of the art and challenges of security SLA for cloud computing", *Computers and Electrical Engineering*, 2017, January.

BBC: "Cuatro claves del cierre de Megaupload", *BBC Mundo (edición digital)*, 2012, noticia de 20.01.2012. Accesible en: http://www.bbc.com/mundo/noticias/2012/01/120119_megaupload_clave_tsb.shtml. Último acceso 08.08.2018.

BERCOVITZ RODRIGUEZ-CANO, Rodrigo: "Comentario al art. 3 de la TRLGDCU", *Comentario del Texto Refundido de la Ley General para la defensa de los consumidores y usuarios y otras leyes complementarias*, 2015, Aranzadi.

BERROCAL LANZAROT, Ana Isabel: "Perfección del contrato en la Ley 24/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico: la unificación de criterios", *Revista de Contratación Electrónica*, 2009, núm. 100.

BLANCO ANTÓN, María José: "Transferencia Internacional de Datos Personales", *Actualidad jurídica Aranzadi*, 2012, nº 836.

BRADSHAW, Simon; MILLARD, Christopher y WALDEN, Ian: "Contracts for Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", *Queen Mary University of London - Legal Studies Research Paper*, 2010, nº 63.

BUSTOS, Gerardo: "Seis obligaciones básicas en el nuevo funcionamiento electrónico de las administraciones públicas", *Actualidad Jurídica Aranzadi*, 2016, Cizur Menor, núm. 923/2016, parte Comentario.

C

CÁMARA LAPUENTE, Sergio: "Artículos 1 a 7", *Comentarios a las normas de protección de los consumidores. Texto refundido (RDL 1/2007) y otras leyes y reglamentos vigentes en España y en la Unión Europea*, 2011, Colex.

CAMPOS ACUÑA, María Concepción: "Implantación de la administración electrónica. 5 lecciones que aprender de la experiencia FACe", *La Administración Práctica*, 2017, Cizur Menor, núm. 5/2017, parte análisis doctrinal.

CARBALLO FIDALGO, Marta: "Ámbito de aplicación del régimen legal sobre cláusulas abusivas", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch.

CARBALLO FIDALGO, Marta: "Consecuencias negociales del carácter abusivo de una cláusula. La nulidad parcial del contrato", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch.

CARBALLO FIDALGO, Marta: "Las cláusulas en todo caso prohibidas (I)", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch.

CARBALLO FIDALGO, Marta: "Las cláusulas en todo caso prohibidas (II)", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch.

CARBALLO FIDALGO, Marta: "Marco normativo. Derecho comunitario e interno", *La protección del consumidor frente a las cláusulas no negociadas individualmente*, 2013, Bosch.

CARRASCO PERERA, Ángel: "Control de validez de condiciones generales y cláusulas abusivas", *Derechos de contratos*, 2017, Aranzadi.

CHOU, David C.: "Cloud computing risk and audit issues", *Computers Standards & Interfaces*, 2015.

CINCO DÍAS (edición digital): "La Ley patriota de EE.UU. castiga a las tecnológicas", 2013, noticia de 17.06.2013. Accesible en: https://cincodias.elpais.com/cincodias/2013/06/16/empresas/1371398022_860080.html. Último acceso: 08.08.2018

CNUDMI – Nota de la Secretaría "A/CN.9/WG.IV/WP.151 - Aspectos contractuales de la computación en la nube - Propuesta de los Estados Unidos de América", 2018, 56º período de sesiones. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V18/003/92/PDF/V1800392.pdf. Último acceso: 08.08.2018.

CNUDMI – Nota de la Secretaría: "A/CN.9/WG.IV/WP.148 - Aspectos contractuales de la computación en la nube", 2018, 56º período de sesiones. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V18/003/92/PDF/V1800392.pdf. Último acceso: 08.08.2018.

CNUDMI – Nota de la Secretaría: "A/CN.9/WG.IV/WP.142 - Aspectos contractuales de la computación en la nube", 2017, 55º período de sesiones. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/LTD/V17/006/45/PDF/V1700645.pdf. Último acceso: 08.08.2018.

CNUDMI: "Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 55º período de sesiones" (Nueva York, 24 a 28 de abril), 2017. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V17/029/31/PDF/V1702931.pdf. Último acceso: 08.08.2018.

CNUDMI: "Informe del Grupo de Trabajo IV (Comercio Electrónico) sobre la labor realizada en su 54º período de sesiones" (Viena, 31 de octubre a 4 de noviembre), 2016. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/097/13/PDF/V1609713.pdf. Último acceso: 08.08.2018.

CNUDMI: "Posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la informática "en la nube" - Propuesta del Gobierno del Canadá", 48º Período de sesiones, 2015. Accesible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V15/040/53/PDF/V1504053.pdf. Último acceso: 08.08.2018

COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA: "Informe sobre la liberación de la computación en la nube en Europa (2013/2063 (INI))", 2013, (24.10.2013). Accesible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//ES. Último acceso: 08.08.2018.

COMISIÓN EUROPEA: "Un mercado único digital para Europa: la Comisión establece 16 iniciativas para conseguirlo" (06.05.2015), 2015. Accesible en: http://europa.eu/rapid/press-release_IP-15-4919_es.htm. Último acceso: 08.08.2018.

COMISIÓN EUROPEA: "Comunicación de la comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Contratación pública electrónica de extremo a extremo para modernizar la administración pública", 2013, COM (2013) 0453 Final. Accesible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52013DC0453. Último acceso: 08.08.2018.

COMISIÓN EUROPEA: "Agenda Digital: Nueva estrategia para impulsar las empresas europeas y la productividad de la administración pública gracias a la computación en nube" (27.09.2012), 2012. Accesible en: http://europa.eu/rapid/press-release_IP-12-1025_es.htm. Último acceso: 08.08.2018.

COMISIÓN EUROPEA: "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Liberar el potencial de la computación en nube en Europa", 2012, COM (2012) 529 final. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2012:0529:FIN. Último acceso: 08.08.2018.

COMISIÓN EUROPEA - COMMISSION STAFF (WORKING PAPER): "Evaluation Report Impact and Effectiveness of EU Public Procurement Legislation", 2011 Accesible en: https://ec.europa.eu/docsroom/documents/15468/attachments/1/translations/en/renditions/pdf. Último acceso: 08.08.2018.

COMISIÓN EUROPEA: "Libro Verde sobre la generalización del recurso a la contratación pública electrónica en la UE", 2010, COM (2010) 0571 Final. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52010DC0571. Último acceso: 08.08.2018.

COMITÉ ECONÓMICO Y SOCIAL EUROPEO: "La computación en nube (*cloud computing*) en Europa" (Dictamen de iniciativa), 2012. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52011IE1606&from=ES. Último acceso: 08.08.2018.

CORA: "Reforma de las Administraciones Públicas", 2013, Ministerio de Hacienda y Administraciones Públicas – Ministerio de la Presidencia. Accesible en: https://administracion.gob.es/pag_Home/dam/jcr:4c4e8573-6220-4b6a-9397-8f95e566b42a/INFORME-LIBRO.pdf. Último acceso: 08.08.2018.

COTINO HUESO, Lorenzo: "Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"". *Revista catalana de dret públic*, 2015, nº 51.

CRUZ RIVERO, Diego: "Contratación electrónica con consumidores", *Revista de Contratación Electrónica*, 2009, nº 109.

CUESTA SAINZ, Carmen; ALONSO, Javier; TUESTA, David; FERNÁNDEZ DE LIS, Santiago: "El desarrollo de la industria del cloud computing: impactos y transformaciones en marcha", *BBVA Research – Observatorio de Economía Digital*, 2014, (04.07.2014). Accesible en: https://www.bbvaresearch.com/publicaciones/el-desarrollo-de-la-industria-del-cloud-computing-impactos-y-transformaciones-en-marcha/. Último acceso: 08.08.2018.

CUNNINGHAM, Alan; y REED, Chris: "Caveat Consumer? – Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud", *Queen Mary University of London - Legal Studies Research Paper*, 2013, nº 130. Accesible en: https://ssrn.com/abstract=2202758. Último acceso: 08.08.2018.

CUNNINGHAM, Alan; y REED, Chris: "Caveat Consumer? – Consumer Protection and Cloud Computing Part 2 – The Application of ex ante and ex post Consumer Protection Law in the Cloud", *Queen Mary University of London - Legal Studies Research Paper*, 2013, nº 133. Accesible en: https://ssrn.com/abstract=2212051. Último acceso: 08.08.2018.

CUNY, Delphine: "Le cloud à la française, histoire d'un flop?", *LaTribune.fr* , 2015 (13.01.2015). Accesible en: http://www.latribune.fr/technos-medias/informatique/20150113triba29598d73/le-cloud-a-la-francaise-histoire-d-un-flop.html. Último acceso: 08.08.2018.

D

DÁVARA RODRÍGUEZ, Miguel Ángel: "Los contratos informáticos", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi.

DÁVARA RODRÍGUEZ, Miguel Ángel: "El comercio electrónico y la contratación electrónica", *Manual de Derecho Informático*, 2008, Thomson-Aranzadi.

DE MIGUEL ASENSIO, Pedro Alberto: "Contratación electrónica", *Derecho Privado de Internet*, 2011, Civitas-Thomson Reuters.

DÍAZ BRITO, Francisco Javier: "Contratación electrónica: ¿Camino del laberinto?", *Boletín Aranzadi Civil-Mercantil*, 2001, núm. 23/2001.

DÍAZ DÍAZ, Efrén: "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones". *Revista Aranzadi Doctrinal*, 2016, núm. 6/2016.

DÍEZ-PICAZO Y PONCE DE LEÓN, Luis: "La forma y la documentación del contrato", *Fundamentos del Derecho Civil Patrimonial*, 2012, Civitas, Vol.I.

DIEZ-PICAZO Y PONCE DE LEÓN, Luis: *La Prescripción Extintiva - en el Código civil y en la jurisprudencia del Tribunal Supremo (estudios y comentarios de legislación)*, 2007, Civitas.

DIEZ-PICAZO, Luis: "La protección del Derecho de crédito lesionado y las relaciones obligatorias sinalagmáticas", *Fundamentos del Derecho Civil Patrimonial*. Volumen II: las relaciones obligatorias, 2007, Thomson.

DIRECCIÓN GENERAL PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA: "Guía de aplicación de la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las AA.PP. españolas", *Ministerio de Política Territorial y Administración*

Pública. Secretaría General Técnica, 2011. Accesible en: http://www.sefp.minhafp.gob.es/dam/es/web/publicaciones/centro_de_publicaciones_de_la_sgt/GUIAS_NTI/text_es_files/Guia_conex-red-AA-PP-esp-INTERNET.pdf. Último acceso: 08.08.2018

DLA PIPER UK LLP - COMISIÓN EUROPEA: "Comparative study on cloud computing contracts", 2015. Accesible en: http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/. Último acceso: 08.08.2018.

E

ELDERECHO.com: "Conclusiones de la Sesión sobre el Nuevo Estándar de Seguridad y Privacidad en Cloud Computing: ISO 27018", *LEFEBVRE – EL DERECHO,* 2015. Accesible en: http://tecnologia.elderecho.com/tecnologia/privacidad/fide-cloud_computing-iso_27018-estandar_de_seguridad_y_privacidad_0_772125190.html. Último acceso: 08.08.2018.

ELDIARIO.ES: "La justicia francesa condena a Twitter por incluir cláusulas abusivas para hacer negocio con los datos personales", *eldiario.es*, 2018, noticia de 10.08.2018. Accesible en: https://www.eldiario.es/tecnologia/justicia-francesa-Twitter-clausulas-personales_0_801770541.html. Último acceso: 10.08.2018.

ENISA: "Procure Secure: A guide to monitoring of security service levels in cloud contracts", 2012 (April). Accesible en: https://www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport. Último acceso: 08.08.2018.

ENISA: "Computación en la nube: Beneficios, riesgos y recomendaciones para la seguridad de la información", 2009. Accesible en: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file. Último acceso: 08.08.2018.

ETSI: "Cloud Standards Coordination - Final Report", 2013, November, version 1.0. Accesible en: https://ec.europa.eu/digital-single-market/en/news/cloud-standards-coordination-final-report. Último acceso: 08.08.2018.

EUROPA PRESS: "Apple, Facebook y Google avisarán cuando el Gobierno de EEUU pretenda acceder a datos", *El Mundo.es (edición digital)*, 2014, noticia de 05.05.2014. Accesible en: http://www.elmundo.es/tecnologia/2014/05/05/53676c38e2704eb0068b4579.html. Último acceso: 08.08.2018.

F

FABEIRO SANZ, Jorge: "Guía de la Red Sara. La Administración de mañana, hoy", *Dirección General para el impulso de la Administración Electrónica*, 2008.

FedRAMP: "Guide to Understanding FedRAMP", 2013, v.1.2. Accesible en: https://www.gsa.gov/cdnstatic/Guide_to_Understanding_FedRAMP_042213.pdf. Último acceso: 08.08.2018.

FERNÁNDEZ ALLER, Celia: "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)", *Revista de Derecho UNED*, 2012, núm. 10. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/11093/10621. Último acceso: 08.08.2018.

FERRER RIBA, Josep: "Disposición Adicional Primera. Seis. 2ª", *Comentarios a la Ley sobre Condiciones Generales de Contratación*, 2002, Civitas.

FROSINI, Vittorio: *Informatica, diritto e società*, 1992, Giuffrè.1

G

GALÁN CORONA, Eduardo: "Contrato de servicios mercantiles y contrato de servicios electrónicos en el Anteproyecto de Código Mercantil", *Hacia un Nuevo Código Mercantil,* 2014, Thomson Reuters Aranzadi.

GARCÍA DE PABLOS, Jesús Félix: "La transferencia de datos fuera de la Unión Europea", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2016, núm. 40.

GARCÍA DEL POYO VIZCAYA, Rafael: "Cloud computing: aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, 2012.

GARCÍA DEL POYO VIZCAYA, Rafael: "La contratación empresarial de servicios de cloud computing", *Derecho y Cloud computing*, 2012, Thomson Reuters.

GARCÍA MEXÍA, Pablo: "Cloud computing: sus implicaciones legales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2010, nº 23.

GARCÍA MEXÍA, Pablo: "El comercio electrónico. La regulación de contenidos", *Derecho europeo de internet. Hacia la autonomía académica y la globalidad geográfica*, Netbiblo, 2009.

GARCÍA SÁNCHEZ, Manuel: "Retos de la computación en la nube", *Derecho y Cloud computing*, 2012.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Directrices sobre los delegados de protección de datos (DPD)", 2016, 16/ES, WP 243 rev.01 (13.12.2016). Accesible en: https://www.aepd.es/media/criterios/wp243rev01-es.pdf. Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", 2015, 2588/15/EN, WP 232 (22.09.2015). Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf. Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos", 2014, 1471/14/ES, WP 223 (16.09.2014). Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf. Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Dictamen 05/2012 sobre la computación en nube", 2012, 01037/12/ES, WP 196 (01.07.2012). Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf. Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", 2012, 00930/12/EN WP 195 (06.06.2012)", 2012. Accesible en: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49726. Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC", 2010, 00070/2010/EN, WP176 (12.07.2010). Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf. Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»", 2010, 00264/10/ES, WP 169 (16.02.2010). Accesible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf . Último acceso: 08.08.2018.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29: "Documento de Trabajo Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", 1998, DG XV D/5025/98, WP 12 (24.07.1998). Accesible en:

http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf. Último acceso: 08.08.2018.

GUASCH PORTAS, Vicente: "La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE", *Revista de Derecho UNED*, 2017, nº 20.

GUASH PORTAS, Vicente y SOLER FUENSANTA, José Ramón: ""Cloud computing": cláusulas contractuales y reglas corporativas vinculantes", *Revista de Derecho UNED*, 2014, núm. 14. Accesible en: http://revistas.uned.es/index.php/RDUNED/article/view/13300. Último acceso: 08.08.2018.

GUTIÉRREZ, Horacio E. y KORN, Daniel: "Facilitando "the cloud": la regulación de la protección de datos como motor de la competitividad nacional en América latina", *Revista la propiedad inmaterial*, 2014, nº 18.

H

HERNANDEZ DE ROJAS, Félix: "Fog computing: motor de innovación para el mundo IoT", *A un clic de las Tic*, Telefónica, 2015 (4.02.2015). Accesible en: http://www.aunclicdelastic.com/fog-computing-motor-de-innovacion-para-el-mundo-iot/. Último acceso: 08.08.2018

HERNÁNDEZ JIMÉNEZ-CASQUET, Fernando: "El marco jurídico del comercio y la contratación electrónicos", *Principios de Derecho de internet*, Tirant lo Blanch, 2005.

HON, W Kuan; MILLARD, Christopher y WALDEN, Ian: "Negotiating Cloud Contracts – Looking at Clouds from Both Sides Now", *Queen Mary University of London - Legal Studies Research Paper*, 2012, nº 117.

I

ILLESCAS ORTIZ, Rafael: "Los principios generales del Derecho del comercio electrónico", *Derecho de la Contratación Electrónica*, 2009, Civitas,

INFORMATION COMMISSIONER'S OFFICE (ICO, UK): "Guidance on the use of cloud computing: Data protection act 1998", 2012, v. 1.1.

INTECO: "Estudio sobre el *cloud computing* en el sector público en España", 2012. Accesible en: https://www.scribd.com/document/99564543/Estudio-sobre-cloud-computing-en-el-sector-publico-en-Espana. Último acceso: 08.08.2018

ITBusinessEDGE (Blog): "How the Internet of Things Will Transform the Data Center". Accesible en: http://www.itbusinessedge.com/slideshows/how-the-internet-of-things-will-transform-the-data-center-08.html. Último acceso: 08.08.2018.

J

JANSEN, Wayne y GRANCE, Timothy: "Guidelines on Security and Privacy in Public Cloud Computing", *National Institute of Standards and Technology, US. Department of Commerce*, 2011. Accesible en: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. Último acceso: 08.08.2018.

JONES, Steve: "Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study", *International Journal of Information Management*, 2015, Volume 35, Issue 6.

K

KUNDRA, Vivek: "Federal Cloud computing strategy", *The White House – Washington*, 2011. Accesible en: https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf. Último acceso: 08.08.2018.

L

LESSIG, Lawrence: "El código y otras leyes del ciberespacio", 2001, Taurus.

LÓPEZ JIMÉNEZ, David: "Consideraciones de carácter general relativas al comercio electrónico: vino nuevo sobre odres viejos", *Nuevas coordenadas para el Derecho de obligaciones. La autodisciplina del comercio electrónico*, 2013, Marcial Pons.

LÓPEZ JIMÉNEZ, David: "La "computación en la nube" o "cloud computing" examinada desde el ordenamiento jurídico español", *Revista de Derecho*, 2013, nº 40.

LÓPEZ JIMÉNEZ, David: "Los sistemas de autodisciplina: presupuestos para su concurrencia", *Nuevas coordenadas para el Derecho de obligaciones. La autodisciplina del comercio electrónico*, 2013, Marcial Pons.

LUNA, Jesús; SURI, Neeraj; IORGA, Michaela; y KARMEL, Aniel: "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards", *IEEE Cloud Computing*, 2015, vol. 2.

LYNDERSAY, Mark: "Microsoft evangelises the cloud", *Guardian (edición digital)*, 2012, noticia de 25.10.2012. http://www.guardian.co.tt/business-guardian/2012-10-24/microsoft-evangelises-cloud. Ultimo acceso: 08.08.2018.

M

MADRID PARRA, Agustín: "Tipificación de contratos para las comunicaciones electrónicas en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295.

MADRID PARRA, Agustín: "Contratos electrónicos y contratos informáticos", *Revista de Contratación Electrónica*, 2011, núm. 111.

MADRID PARRA, Agustín: "Tramitación y contenido de la Ley Modelo de la CNUDMI/UNCITRAL sobre las firmas electrónicas", *El contrato por medios electrónicos*, 2003, Universidad Externado de Colombia.

MADRID PARRA, Agustín: "Aspectos jurídicos de la identificación en el comercio electrónico", *Derecho del comercio electrónico*, 2001.

MAQUERIRA MARÍN, Juan Manuel y BRUQUE CÁMARA, Sebastián: "Agentes impulsores de la adopción de cloud computing en las empresas. ¿Quién mueve la nube?", *Universia Business Review*, 2012.

MARÍN LÓPEZ, Juan José: "El ámbito de aplicación de la Ley sobre condiciones generales de la contratación", *Condiciones Generales de la Contratación y Cláusulas Abusivas*, 2000, Lex Nova.

MARTÍNEZ, Manuel: "Cloud computing y la Administración Pública", Boletic, 2011, nº 60 Accesible en: http://www.astic.es/sites/default/files/boletic_completos/boletic_60_completo.pdf. Último acceso: 08.08.2018.

MARTÍNEZ, Ricard: "Las medidas de seguridad en el Reglamento general de protección de datos", *LOPD y Seguridad* (blog personal), 2016, entrada de 20.12.2016. Accesible en: http://lopdyseguridad.es/gdpr1/. Último acceso: 08.08.2018.

MARTÍNEZ FERREIRO, Susana: "La convergencia de cloud pública e híbrida dará paso a entornos multicloud", *A un clic de las Tic*, Telefónica, 2015 (14.07.2015). Accesible en: http://www.aunclicdelastic.com/la-convergencia-de-cloud-publica-e-hibrida-dara-paso-a-entornos-multicloud/. Último acceso: 08.08.2018.

MARTÍNEZ GUTIÉRREZ, Rubén: "El uso de los medios electrónicos en la contratación pública. La relación entre las Leyes 39 y 40 de 2015 y las Directivas 24 y 55 de 2014 de contratación pública y facturación electrónica. Propuestas para tu transposición", *La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho*, 2017, INNAP Investiga.

MARTOS, Natalia: "Se acerca el 25 de mayo de 2018. ¿Está su empresa adaptada al nuevo Reglamento de Protección de Datos?, *Diario La Ley*, 2017, núm. 9081, sección Tribuna.

MARZO PORTERA, Ana María: "Privacidad y cloud computing, hacia dónde camina Europa". *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, 2012, nº 8.

MARZO PORTERA, Ana y MARZO PORTERA, Iziar: "Definición de los contratos informáticos y electrónicos", *Los Contratos Informáticos y Electrónicos. Guía práctica y formularios*, 2004, Ediciones Experiencia S.L.

MAS BADÍA, María Dolores: "El contrato electrónico de seguro", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2015, núm. 38.

MENDOZA LOSANA, Ana Isabel: "Control de condiciones generales de la contratación en sectores regulados. En particular, la cláusula que permite la modificación unilateral de los precios", *Centro de Estudios de Consumo*, 2013. Accesible en: https://ruidera.uclm.es/xmlui/handle/10578/8818. Último acceso: 08.08.2018.

MENÉNDEZ MATO, Juan Carlos: "Aspectos teóricos: Concepto. Validez y clasificación", *El contrato vía Internet*, 2005, J.M. Bosch editor.

MENÉNDEZ MATO, Juan Carlos: "Perspectiva espacio-temporal: La conclusión del contrato desde Internet", *El contrato vía Internet*, 2005, J.M. Bosch editor.

MERCHÁN MURILLO, Antonio: "Cloud computing: soluciones ante un posible conflicto de leyes", *Revista La Ley Mercantil*, 2018, nº48, junio 2018.

MICROSOFT AZURE: "City of Barcelona - City Deploys Big Data BI Solution to Improve Lives and Create a Smart-City Template", 2013. Accesible en: https://azure.microsoft.com/es-es/case-studies/customer-stories-barcelona/. Último acceso: 08.08.2018.

MINISTERIO DE ECONOMÍA Y EMPRESA – MINISTERIO DE HACIENDA (GOBIERNO DE ESPAÑA): "Plan de Servicios Públicos Digitales", 2014, junio. Accesible en: http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaserviciospublicos/Detalle%20del%20Plan/Plan-ADpE-8_ServiciosP%C3%BAblicos.pdf. Último acceso: 08.08.2018.

MINISTERIO DE ECONOMÍA Y EMPRESA – MINISTERIO DE HACIENDA (GOBIERNO DE ESPAÑA): "Plan de impulso de la economía digital y los contenidos digitales", 2013, junio. Accesible en: http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecacontenidos/Detalle%20del%20Plan/Plan-ADpE-3_Contenidos.pdf. Último acceso: 08.08.2018.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS – CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA: "Aprobadas las líneas estratégicas del plan de Administración Electrónica del Gobierno 2013-2015", 2013, nota de prensa del 15.01.2013. Accesible en: http://www.minhafp.gob.es/Documentacion/Publico/GabineteMinistro/Notas%20Prensa/2013/S.E.%20ADMINISTRACIONES%20PUBLICAS/15-01-13%20NP%20CS%20Administraci%C3%B3n%20Electr%C3%B3nica.pdf. Último acceso: 08.08.2018.

MONTÉS PENADÉS, Vicente: "La Defensa del Derecho de Crédito", *Derecho Civil – Derecho de obligaciones y contratos*, 2001, Tirant lo Blanch.

MORALES, José Ramón: "Cloud computing: Riesgos corporativos e implicaciones jurídicas", *Actualidad jurídica Aranzadi*, 2013, nº 863.

MORENO, Víctor: "La UE solicita que Whatsapp interrumpa el intercambio de datos con Facebook", *Expasión.com*, 2016, noticia de 28.10.2016. Accesible en: http://www.expansion.com/economia-digital/companias/2016/10/28/58133c5bca4741c87f8b45a2.html. Último acceso: 08.08.2018.

MORENO NAVARRETE, Miguel Ángel: "Los fundamentos del contrato electrónico", *DERECHO-e Derecho del Comercio electrónico*, 2002, Marcial Pons.

MÚGICA ARRIEN, Gotzone: "Los contratos informáticos", SABERES, revista de estudios jurídicos, económicos y sociales, 2003, Universidad Alfonso X El Sabio, Vol. 1. Accesible en: https://revistas.uax.es/index.php/saberes/article/view/687. Último acceso: 08.08.2018.

N

NATIONAL CYBER SECURITY CENTRE (UK): "Guidance – Implementing the Cloud Security Principles", 2016. Accesible en: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles. Último acceso: 08.08.2018.

NAVAS NAVARRO, Susana: "Computación en la nube: Big Data y protección de datos personales", InDret, 2015, vol. 4. Accesible en: http://www.indret.com/pdf/1193_es.pdf. Último acceso: 08.08.2018.

NIST: "The NIST Definition of Cloud Computing", 2011. Accesible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Último acceso: 08.08.2018.

O

OBSAE: "Hacia una estrategia de Cloud Computing en las Administraciones Públicas", *Notas técnicas*, 2013, febrero. Accesible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:99490b88-c2d4-4ca1-b16e-140fa7caf13c/2013-02_nota_tecnica_CLOUD.pdf. Último acceso: 08.08.2018.

OBSERVATORIO CETELEM: "La era del "marketplace"", *eCommerce*, 2017.

ONTSI: "Cloud Computing. Retos y Oportunidades", *Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información* , 2012. Accesible en: http://www.ontsi.red.es/ontsi/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf. Último acceso: 08.08.2018.

ORDUÑA MORENO, Javier: "Extinción de la obligación", *Derecho Civil – Derecho de obligaciones y contratos*, 2001, Tirant lo Blanch.

P

PAEZ, Mauricio; VON DIEMAR, Undine; LITTLE, Jonathon; ROBERTSON, Elizabeth; BRU, Paloma; HAAS, Olivier; y DE MUYTER, Laurent: ""EU-U.S. Privacy Shield" to replace "Safe Harbor"", *Jones Day Publications*, 2016. Accesible en: http://www.jonesday.com/eu-us-privacy-shield-to-replace-safe-harbor-02-04-2016/. Último acceso: 08.08.2018.

PAGADOR LÓPEZ, Javier: "Condiciones generales y cláusulas abusivas", *La defensa de los consumidores y usuarios (comentario sistemático del Texto Refundido aprobado por Real Decreto Legislativo 1/2007),* 2011, Iustel.

PAGADOR LÓPEZ, Javier: "Requisitos de incorporación de las condiciones generales", *Condiciones Generales de la Contratación y Cláusulas Abusivas*, 2000, Lex Nova.

PALOMAR I BAGET, Jesús: "Cómo empezar a utilizar herramientas en la nube en nuestra administración", *Redes sociales y herramientas en la nube para las administraciones públicas del siglo XXI*, 2014. En: http://www.eudel.eus/es/archivos/libro/redes_socilaes_y_herramientas.pdf. Último acceso: 08.08.2018

PALOMAR OLMEDA, Alberto: "El paradigma del cambio: la transformación tecno", *Actualidad Jurídica Aranzadi*, 2016, Cizur Menor, núm. 920/2016, parte Tribunal.

PALOMAR OLMEDA, Alberto: "Incidencia del cloud computing en el ámbito de la contratación pública", *Derecho y cloud computing*, 2012.

PARDO GATO, José Ricardo: "Las condiciones generales de la contratación y el listado de cláusulas abusivas", *Las cláusulas abusivas en los contratos de adhesión*, 2004, Dijusa.

PARLAMENTO EUROPEO (Nota de prensa): "Suspend EU-US data exchange deal, unless US complies by 1 September, say MEPs", 2018, nota de 05 de julio de 2018. Accesible en: http://www.europarl.europa.eu/news/es/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps. Último acceso: 08.08.2018.

PEDRAZA CÓRDOBA, Juanita: "Los riesgos sobre la privacidad de los datos personales en un entorno cloud computing: una aproximación desde el reglamento europeo de protección de datos", *Revista de Privacidad y Derecho Digital*, 2017.

PERALES VISCASILLAS, Pilar: "La contratación electrónica en el Anteproyecto de Código Mercantil", *Revista de Derecho Mercantil*, 2015, núm. 295.

PÉREZ ESCOLAR, Marta: "Incorporación al contrato de cláusulas no negociadas: perspectivas de reforma a la luz del panorama europeo, la Propuesta de Modernización del Código civil y el Anteproyecto de Ley de Código mercantil", *Anuario de Derecho Civil,* 2015, Vol. 68, nº 2.

PERTÍÑEZ VÍLCHEZ, Francisco: "Buena fe ex art. 1.258 cc y nulidad de las cláusulas suelo sorpresivas en contratos de préstamo con adherentes empresarios", *Indret: Revista para el Análisis del Derecho*, 2016, número 4, p. 12. Accesible en: http://www.indret.com/pdf/1266_es.pdf. Último acceso: 08.08.2018.

PINHEIRO, Marcos: "Catalá oculta que el fallo de LexNET propició más de 400 descargas de documentos confidenciales", *eldiario.es*, 2017, noticia de 12.11.2017. Accesible en: http://www.eldiario.es/politica/Catala-descargas-ilegales-documentos-LexNET_0_706579756.html. Último acceso: 08.08.2018.

PLAZA PENADÉS, Javier: "El Proyecto de la nueva Ley Orgánica de Protección de Datos de Carácter Personal", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2018, núm. 46.

PLAZA PENEDÉS, Javier: "El marco jurídico de la contratación electrónica", *Comercio, Administración y Registros Electrónicos*, 2009, Thomson Reuters.

PLAZA PENADÉS, Javier: "La responsabilidad civil de los intermediarios en internet y otras redes", *Contratación y comercio electrónico*, 2003.

PRIETO, Miriam: "Amazon, Microsoft, Google e IBM libran la gran batalla del 'cloud computing'", *Expasión.com*, 2016, noticia de 01.11.2016. Accesible en: http://www.expansion.com/economia-digital/companias/2016/11/01/581381d8e5fdea8e3e8b4587.html. Último acceso: 08.08.2018.

PUYOL, Javier: "Especial consideración de la Evaluación de Impacto en el Reglamento General de Protección de Datos de la Unión Europea (RGPDEU) y en sus normas de desarrollo", *El modelo de evaluación de riesgos en la protección de datos EIPD/PIA's*, 2018, Tirant lo Blanch.

Q

QUINTANA, Eduardo: "Amazon alojará en Canadá un data center para la nube", *MCPRO muycomputerpro.com*, 2016 (15.01.2016). Accesible en: http://www.muycomputerpro.com/2016/01/15/amazon-alojara-en-canada-un-data-center-para-la-nube . Último acceso: 08.08.2018.

R

RAMOS SUÁREZ, Álvaro: "Novedades de 2016 en materia de Privacidad y Ciberseguridad", *Actualidad Jurídica Aranzadi*, 2016, núm. 923/2016.

RECALDE CASTELLS, Andrés: "Comercio y Contratación electrónica", *Informática y Derecho – Revista Iberoamericana de Derecho informático*, 1999, núm. 30-31-32.

REGLERO CAMPOS, Luis Fernado: "ARTS. 744-773; 1278-1280; 1961-1975", *Jurisprudencia Civil comentada*, 2000, Comares.

RENGIFO GARCÍA, Ernesto: "Computación en la nube", *Revista La Propiedad Inmaterial*, 2013, nº 17.

RODRÍGUEZ, Sergio: "El FBI cierra Megaupload, una de las mayores webs de intercambio de archivos", *El Mundo.es (edición digital)*, 2012, noticia de 20.01.2012. Accesible en: http://www.elmundo.es/elmundo/2012/01/19/navegante/1327002605.html. Ultimo acceso: 08.08.2018

RODRÍGUEZ DE LAS HERAS BALLELL, Teresa: "Intermediación en la red y responsabilidad civil", *Revista Española de Seguros*, 2010, núm. 142.

ROMAN LLAMOSI, Sofía: "Los contratos bancarios – Aumento litigiosidad y respuesta de los tribunales", *Revista de Derecho vLex*, 2015, núm. 131

ROSSELLÓ RUBERT, Francisca María: "Concepto y características técnicas del *Cloud Computing*", *Cloud Computing. Régimen Jurídico para Empresarios*, 2018, Thomson Reuters Aranzadi.

ROSSELLÓ RUBERT, Francisca María: "Modificación, suspensión y extinción del contrato de Cloud Computing", *Cloud computing. Régimen Jurídico para Empresarios*, 2018, Thomson Reuters Aranzadi.

ROYO MARTÍNEZ, Miguel: "Contratos de Adhesión", *Anuario de Derecho Civil*, 1949. Accesible en: https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-C-1949-10005400070_ANUARIO_DE_DERECHO_CIVIL_Contratos_de_adhesi%F3n. Último acceso: 08.08.2018.

RUBÍ NAVARRETE, Jesús: "El proveedor de cloud como encargado del tratamiento". *Derecho y Cloud computing*, 2012.

S

SÁNCHEZ DEL CASTILLO, Vilma: "Algunas referencias sobre los aportes del Doctor Rafael Illescas Ortiz al Derecho del Comercio electrónico. A propósito de la regulación estatuida en el capítulo de contratación electrónica de la propuesta de Código Mercantil", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, 2015, Universidad Carlos III de Madrid.

SÁNCHEZ LEIRA, Reyes: "Contrato de hospedaje en página web: estructura contractual básica y protección de datos", *Revista de Contratación Electrónica*, 2005, núm. 61.

SILICON: "Amazon abrirá un primer centro de datos de almacenamiento en la nube en Canadá", 2016 (14.01.2016). Accesible en: http://www.silicon.es/amazon-abrira-un-primer-centro-de-datos-de-almacenamiento-en-la-nube-en-canada-2299783. Último acceso: 08.08.2018.

T

TECNOXPLORA: "El Ministerio de Justicia denuncia al hacker que descubrió el fallo en LexNET", *laSexta.com*, 2018, noticia de 08.02.2018. Accesible en: http://www.lasexta.com/tecnologia-tecnoxplora/internet/ministerio-justicia-denuncia-hacker-que-descubrio-fallo-lexnet_20170808598994980cf2c0f4137e4fd5.html. Último acceso: 08.08.2018.

THE GUARDIAN: "NSA paid millions to cover Prism compliance costs for tech companies", *TheGuardian.com,* 2013, noticia de 23.08.2013. Accesible en: https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid. Último acceso: 08.08.2018.

TIMBERG, Craig: "Apple, Facebook, others defy authorities, increasingly notify users of secret data demands after Snowden revelations", *The Whashington Post (digital)*, 2014, noticia de 01.05.2014. Accesible en: http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html?hpid=z1. Último acceso: 08.08.2018.

TUR FAÚNDEZ, María Nélida: "La responsabilidad contractual de los intermediarios electrónicos", *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, Comares, 2005.

U

UK GOVERNMENT G-CLOUD: "G-Cloud buyers' guide", 2018. Accesible en: https://www.gov.uk/guidance/g-cloud-buyers-guide. Último acceso: 08.08.2018.

UK GOVERNMENT G-CLOUD: "G-Cloud suppliers' guide", 2018. Accesible en: https://www.gov.uk/guidance/g-cloud-suppliers-guide. Último acceso: 08.08.2018.

UK GOVERNMENT G-CLOUD: "Guidance - How to award a contract when you buy services", 2018. Accesible en: https://www.gov.uk/guidance/how-to-award-a-contract-when-you-buy-services. Último acceso: 08.08.2018.

V

VALERO TORRIJOS, Javier: "Una lección del pasado: los problemas e insuficiencias derivados de las opciones de transposición por parte del legislador español", *La transposición en España de la normativa europea sobre contratación pública electrónica: una oportunidad para la innovación tecnológica*, 2015, La Nueva Contratación Pública. Accesible en: http://www.obcp.es/index.php/mod.documentos/mem.descargar/fichero.documentos_La-nueva-contratacion-publica_e813ae7b%232E%23pdf/chk.cdd19408e57c2bf2e92eb186d7786d1b. Último acceso: 08.08.2018.

VALLE, Teresa: "Los gobiernos pueden migrar a la nube con confianza", *New Center Latinoamérica,* Microsoft, 2016 (28.01.2016). Accesible en: http://news.microsoft.com/es-xl/features/los-gobiernos-pueden-migrar-a-la-nube-con-confianza. Último acceso: 08.08.2018.

VANROEKEL, Steven: "Security Authorization of Information Systems in Cloud Computing Environments", 2011. Accesible en: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/fedrampmemo.pdf. Último acceso: 08.08.2018.

VEGA VEGA, José Antonio: "Las condiciones generales en la contratación electrónica", *Revista de Contratación Electrónica*, 2009, nº 101.

VILALTA NICUESA, Aura Esther: "Resolución electrónica de conflictos", *Principios de Derecho de la Sociedad de la Información*, 2010, Aranzadi-Thomson Reuters.

VVAA: "Nuevo Estándar de Seguridad y Privacidad en Cloud Computing: ISO 27018", *FIDE (Fundación para la Investigación sobre el Derecho y la Empresa)*, 2014, conferencia 12.12.2014. Accesible en: http://www.fidefundacion.es/Resumenes-de-sesiones-y-foros_a170.html. Último acceso: 08.08.2018.

W

WALT, Vivienne: "Barcelona: The most wired city in the world", *Fortune (web)*, 2015, publicación de 29.07.2015. Accesible en: http://fortune.com/2015/07/29/barcelona-wired-city/. Último acceso: 08.08.2018.

RECURSOS ELECTRÓNICOS ANALIZADOS[792]

A3 SOFTWARE

Condiciones particulares del contrato de servicios Cloud, versión a 08.08.2018. Accesible en: https://media.a3software.com/cloud/Condiciones%20particulares%20contrato%20servicios%20cloud.pdf. Último acceso: 08.08.2018.

ACENS

Condiciones Generales de Contratación electrónica y telefónica de servicios ACENS, versión 08.08.2018. Accesible en: https://www.acens.com/file_download/condiciones_generales_de_contratacion_electronica_acens.pdf. Último acceso: 08.08.2018.

Condiciones Particulares del servicio SMART IB, versión 08.08.2018. Accesible en: https://www.acens.com/file_download/Condiciones_particulares_de_Servicio_Smart_Bi.pdf. Último acceso: 08.08.2018.

Contrato de tratamiento de datos para servicios de alojamiento, versión 08.08.2018. Accesible en: https://www.acens.com/file_download/contrato_tratamiento_de_datos_personales.pdf. Último acceso: 08.08.2018.

ADOBE

Condiciones Adicionales de Uso para DOCUMENT CLOUD, versión 16.06.2016. Accesible en: http://www.adobe.com/content/dam/acom/es/legal/servicetou/Document-Cloud_Additional_TOU-es_ES_20160616.pdf. Último acceso: 08.08.2018.

ADRIVE

Terms of Service, versión 22.09.2015. Accesible en: http://www.adrive.com/terms. Último acceso: 08.08.2018.

AMAZON

Condiciones de Uso de Amazon Drive, modificación 09.06.2018. Accesible en: https://www.amazon.es/gp/help/customer/display.html?nodeId=201376540. Último acceso: 08.08.2018.

Contrato de Nivel de Servicios para AWS, fecha efectiva 12.02.2018. Accesible en: https://aws.amazon.com/es/compute/sla/. Último acceso: 08.08.2018.

Customer Agreement de AWS, fecha de última actualización 01.07.2018. Accesible en: https://aws.amazon.com/es/agreement/. Último acceso: 08.08.2018

Overview of Security Processes para AWS, version 05.2017. Accesible en: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf . Último acceso: 08.08.2018.

Overview of Security Processes para AWS, version de 09.2013. Derogado.

Site Terms, versión 23.12.2011. Accesible en: https://aws.amazon.com/es/terms/. Último acceso: 08.08.2018.

[792] Salvo que expresamente se indique, los recursos electrónicos seleccionados están vigentes a fecha de 08.08.2018. Las licitaciones de las Instituciones públicas analizadas, de RED.es y Patrimonio Nacional, indican la fecha de publicación de los documentos analizados y su enlace de acceso.

APONTE SYSTEMS

Política de Uso Justo (AUP), versión 3.1.8E. Accesible en: https://aponte-systems.com/secure/Politicas/Uso_Aceptable. Último acceso: 08.08.2018.

APPLE

iCloud Términos Y Condiciones, versión 19.09.2017. Accesible en: https://www.apple.com/legal/internet-services/icloud/es/terms.html. Último acceso: 08.08.2018

iWork.com Public Beta Condiciones de Servicio, revisión 19.01.2010. Accesible en: https://www.apple.com/legal/iworkcom/es/terms.html. Último acceso: 08.08.2018.

ARSYS

Condiciones específicas para CLOUDBUILDER NEXT. Condiciones a fecha de 08.08.2018 (Ref.: CECBN_141217). Accesible en: https://www.arsys.es/legal?dhtml=contrato-ngcs. Último acceso: 08.08.2018.

Condiciones generales de Servicio. Condiciones a fecha de 08.08.2018 (Ref.: CGS_23052018). Accesible en: https://www.arsys.es/legal?dhtml=condiciones-generales-contratacion. Último acceso: 08.08.2018.

BOX

Términos de Servicio, desde 01.08.2017. Accesible en: https://www.box.com/es-419/legal/termsofservice. Último acceso: 08.08.2018.

CLARANET

Condiciones Particulares del Servicio de VDC. Actualizadas en octubre de 2016 (vigentes). Accesible en: https://www.claranet.es/legal/condiciones-particulares-de-los-servicios-de-vdc. Último acceso: 08.08.2018.

CLOUD DRIVE

Term of Service, versión a 08.08.2018. Accesible en: https://www.driveoncloud.com/term.html. Último acceso: 08.08.2018.

DATAPIPE

Purchase order terms and conditions, versión de 22.05.2017. No se puede realizar nueva contratación del servicio, aplicable solo para clientes con contrato.

DROPBOX

Business Agreement, fecha de publicación 17.04.2018. Accesible en: https://www.dropbox.com/terms#business_agreement. Último acceso: 08.08.2018.

Business Agreement, fecha de revisión 30.01.2017. Derogado.

Condiciones de Servicio, fecha de publicación 17.04.2018. Accesible en: https://www.dropbox.com/privacy#terms. Último acceso: 08.08.2018.

Política de seguridad. Vigente a 08.08.2018. Accesible en: https://www.dropbox.com/business/trust/security/architecture. Último acceso: 08.08.2018

Política de seguridad. Vigente a 20.12.2016. Derogada.

Política de seguridad. Vigente a 14.09.2013. Derogada.

Política de Transferencia de datos entre Europa y Estados Unidos. Vigente a 08.08.2018. Accesible en: https://www.dropbox.com/help/security/data-transfers-europe-us. Último acceso: 08.08.2018.

Whitepaper, versión v2017.04. Accesible en: https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf. Último acceso: 08.08.2018.

FACEBOOK

Condiciones del Servicio, fecha de revisión 19.04.2018. Accesible en: https://www.facebook.com/legal/terms/update o https://www.facebook.com/legal/terms/plain_text_terms Últimos accesos: 08.08.2018.

Declaración de Derechos y Responsabilidades, versión de 30.01.2015. Derogada.

FLEXIANT

Cloud Orchestrator End User Licence Agreement, version FEUL-2013022501. Accesible en: https://www.flexiant.com/support/eula/. Último acceso: 08.08.2018

GOGRID

Terms of Service, revisión de 22.11.2013 (Ref.: CGS_030417)

GOOGLE

Acuerdo de G Suite a través de distribuidor, versión vigente a 08.08.2018. Accesible en: https://gsuite.google.com/intl/es/terms/reseller_premier_terms_ie_es.html. Último acceso: 08.08.2018.

Cloud Storage SLA. Última revisión 20.10.2016. Accesible en: https://cloud.google.com/storage/sla. Último acceso: 08.08.2018.

Condiciones del Servicio de Google, versión de 25.10.2017. Accesible en: https://policies.google.com/terms?hl=es-419. Último acceso: 08.08.2018.

Política de privacidad y condiciones de Google, cómo conserva Google los datos que recoge, versión vigente a 08.08.2018.

Política de privacidad de Google, revisión de 29.08.2016. Derogada.

GRUPO TREVENQUE

Condiciones Generales de Contratación. Accesible en: https://www.trevenque.es/wp-content/uploads/2017/03/01.-condiciones-legales-contratacion.pdf. Último acceso: 08.08.2018.

HOSTALIA

Términos y Condiciones del Contrato, vigente a 08.08.2018. Accesible en: https://www.hostalia.com/contratar/contrato/. Último acceso: 08.08.2018.

HUAWEI

ID User Agreement, versión 01.2018. Accesible en: https://hwid5.vmall.com/CAS/portal/agreements/userAgreement/en-us_userAgreement.html?version=common. Último acceso: 08.08.2018.

IBM

Cloud Services Agreement, versión Z126-6304-US, 03-2018. Accesible en: https://www.ibm.com/support/customer/pdf/csa_us.pdf. Último acceso: 08.08.2018.

Condiciones Generales para Ofertas de Cloud. Versión: i126-5948-02 (01/2017). Accesible en: http://www-03.ibm.com/software/sla/sladb.nsf/pdf/5948-02/$file/i126-5948-02_01-2017_es_ES.pdf. Último acceso: 08.08.2018.

Service Description, IBM Cloud. Versión i126-6605-1 (11/2017). Accesible en: https://www.ibm.com/cloud-computing/bluemix/sites/default/files/assets/docs/i126-6605-12_11-2017_en_US.pdf_0.pdf. Último acceso: 08.08.2018.

MICROSOFT

Contrato de Nivel de Servicio para Azure. Actualización marzo 2018. Accesible en: https://azure.microsoft.com/es-es/support/legal/sla/. Último acceso: 08.08.2018.

Contrato de Nivel de Servicio para Servicios Online de Microsoft, versión española de 01.07.2017. Accesible en: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=12528. Último acceso: 08.08.2018.

Contrato de Servicio de Microsoft, publicación 01.03.2018. Accesible en: https://www.microsoft.com/es-es/servicesagreement/. Último acceso: 08.08.2018.

Contrato de Suscripción Online de Microsoft, versión 04.2018. Accesible en: https://azure.microsoft.com/es-es/support/legal/subscription-agreement/. Último acceso: 08.08.2018.

Contrato de Suscripción Online de Microsoft, versión 09.2013. Derogado.

Security Response in the Cloud para Azure. Actualización 08.02.2017. Accesible en: https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678. Último acceso: 08.08.2018.

Trust center, versión 07.2017. Accesible en: https://www.microsoft.com/es-xl/trustcenter/guidance/risk-assessment. Último acceso: 08.08.2018.

MOVISTAR

Términos y Condiciones particulares del Servicio Movistar Cloud. Vigente a 08.08.2018. Accesible en: http://www.movistar.es/rpmm/estaticos/residencial/fijo/servicios-sobre-adsl/contratos/condiciones-servicio-movistar-cloud.pdf. Último acceso: 08.08.2018.

PATRIMONIO NACIONAL

Pliego de cláusulas administrativas particulares a regir para la contratación del servicio de correo electrónico *SaaS* en la nube de Patrimonio Nacional, publicado el 10.07.2015. Accesible en: https://contrataciondelestado.es/wps/wcm/connect/308e8c58-d909-4e20-9465-deedf76bed87/DOC20150710084936PCAP+512+AIF.pdf?MOD=AJPERES. Último acceso: 08.08.2018.

Pliego de prescripciones técnicas a regir para la contratación del servicio de correo electrónico *SaaS* en la nube de Patrimonio Nacional, publicado el 10.07.2015. Accesible en: https://contrataciondelestado.es/wps/wcm/connect/79b6afc5-2f4d-4480-a725-a1ac8d2bad9e/DOC20150616120720PPT+512+AIF.pdf?MOD=AJPERES

QUERRY S.A.

Condiciones del servicio de backup en la nube, vigente a 08.08.2018 (REF.: jmm100516bn). Accesible en: http://www.querry.com/wp-content/uploads/2015/07/cgbn100516.pdf. Último acceso: 08.08.2018.

RACKSPACE

Cloud SLA, versión 13.08.2018. Accesible en: https://www.rackspace.com/information/legal/cloud/sla. Último acceso: 13.08.2018.

RED HAT OPENSHIFT

Online Services Agreement, versión 02.05.2017. Accesible en: https://www.openshift.com/legal/terms/. Último acceso: 08.08.2018.

RED.ES

Pliego de condiciones generales que regirán la realización del contrato "Remedy en la nube", publicado el 23.02.2018.

Pliego de condiciones particulares que regirán la realización del contrato "Remedy en la nube", publicado el 23.02.2018.

Pliego de prescripciones técnicas que regirán la realización del contrato "Remedy en la nube", publicado el 23.02.2018.

El detalle de la licitación, incluido los tres documentos referidos, se encuentra en https://perfilcontratante.red.es/perfilcontratante/busqueda/DetalleLicitacionesDefault.action;jsessionid=8624DDB536F172DABA2139EAF165ACFB.contratante01?idLicitacion=7005&visualizar=0. Último acceso: 08.08.2018.

SAMSUNG

Términos y condiciones de Samsung Cloud, versión a 08.08.2018. Accesible en: https://account.samsung.com/membership/terms. Último acceso: 08.08.2018.

Términos y condiciones de Samsung Cloud Adicionales, versión a 08.08.2018. Accesible en: https://account.samsung.com/membership/etc/specialTC.do?fileName=personaldatamgmt.html. Último acceso: 08.08.2018.

SAP

Términos y condiciones generales para SAP Cloud Services, versión v.2-2017. Accesible en: https://assets.cdn.sap.com/agreements/general-terms-and-conditions/cls/general-terms-and-conditions-for-sap-cloud-services-direct-spain-spanish-v2-2017.pdf. Último acceso: 08.08.2018.

SEAGATE

Términos y condiciones, versión 03.08.2015. Accesible en: https://www.seagate.com/es/es/legal-privacy/terms-and-conditions/. Último acceso: 08.08.2018.

TERREMARK.ES

Conducta del usuario. Versión 09.2013. Servicio no disponible para nueva contratación.

TPV EN LA NUBE

Condiciones Generales de Contratación. Vigente a 08.08.2018. Accesible en: http://tpvenlanube.com/images/contratos/ContratoClienteTPV.pdf. Último acceso: 08.08.2018.

UKFAST

Privacy Policy, versión 04.07.2018. Accesible en: https://www.ukfast.co.uk/terms/privacy-policy.html. Último acceso: 08.08.2018

Terms and Conditions, versión 07.2017. Accesible en: https://www.ukfast.co.uk/terms/terms-and-conditions.html#setupoption. Último acceso: 08.08.2018.

VELNEO

Condiciones Servicio Velneo Cloud, actualización de enero de 2013. Accesible en: https://velneo.es/politicas/cloud/. Último acceso: 08.08.2018.

SLA, revisión de 08.08.2018. Accesible en: https://doc.velneo.es/sla.html. Último acceso: 08.08.2018

SLA, revisión de 14.05.2014.

VERIZON

Acceptable Use Policy, versión 08.08.2018. Accesible en: http://www.verizonenterprise.com/terms/aup/. Último acceso: 08.08.2018.

WNPOWER

Políticas de Uso Aceptable, versión a 08.08.2018. Accesible en: https://www.wnpower.com/politicas-uso-aceptable-pua/. Último acceso: 08.08.2018.

ZOHO

CREATOR Terms of use, vigente a 08.08.2018. Accesible en: https://www.zoho.com/creator/terms.html. Último acceso: 08.08.2018

Terms of Service para ZOHO, versión de 19.04.2018. Accesible en: https://www.zoho.eu/terms.html. Último acceso: 08.08.2018.

JURISPRUDENCIA

A

AUDIENCIA PROVINCIAL DE BARCELONA: Sentencia 185/2015, de 14 de junio de 2015 (sección 15º). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7499474&links=&optimize=20151022&publicinterface=true. Último acceso: 08.08.2018.

AUDIENCIA PROVINCIAL DE CANTABRIA: Sentencia sobre recurso 452/2014, de 27 de abril de 2015 (Sección 4ª). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7413128&links=&optimize=20150622&publicinterface=true. Último acceso: 08.08.2018.

AUDIENCIA PROVINCIAL DE GUIPÚZCOA: Sentencia sobre recurso 3306/1999, de 12 de junio del 2000 (Sección 3ª). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=2349943&links=Guipuzcoa&optimize=20040524&publicinterface=true. Último acceso: 08.08.2018.

AUDIENCIA PROVINCIAL DE HUELVA: Sentencia sobre recurso 151/2013, de 21 de marzo de 2014 (Sección 3ª). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7039133&links=Huelva&optimize=20140508&publicinterface=true. Último acceso: 08.08.2018.

AUDIENCIA PROVINCIAL DE MÁLAGA: Sentencia sobre recurso 543/2014, de 16 de septiembre de 2016 (Sección 5ª). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7884984&links=&optimize=20161207&publicinterface=true. Último acceso: 08.08.2018.

AUDIENCIA PROVINCIAL DE PONTEVEDRA: Sentencia sobre recurso 118/2017, de 7 de abril de 2017 (Sección 1ª). Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8031891&links=&optimize=20170525&publicinterface=true. Último acceso: 08.08.2018.

J

JUZGADO DE LO MERCANTIL Nº1 DE A CORUÑA: Sentencia 256/2016, de 22 de noviembre de 2016. Accesible en: http://www.poderjudicial.es/stfls/TRIBUNALES%20SUPERIORES%20DE%20JUSTICIA/TSJ%20Galicia/DOCUMENTOS%20DE%20INTERES/Jdo%20Mercantil%201%20A%20Coru%C3%B1a%2022%20nov%202016.pdf. Último acceso: 08.08.2018.

S

SUPREME COURT OF THE UNITED STATES: "United States, petitioner v. Microsoft Corporation, on writ of certiorari to the United States Court of appeals for the second circuit", 2018, 17.04.2018. Accesible en: https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf. Último acceso: 08.08.2018.

T

TRIBUNAL CONSTITUCIONAL: Sentencia 111/2016, de 9 de junio de 2016. Accesible en: http://hj.tribunalconstitucional.es/docs/BOE/BOE-A-2016-6839.pdf. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA: Sentencia de 6 de octubre de 2015, asunto C-362/14. Accesible en: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA: Sentencia de 21 de marzo de 2013, asunto C-92/11. Accesible en: http://curia.europa.eu/juris/celex.jsf?celex=62011CJ0092&lang1=es&type=TXT&ancre. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA: Sentencia de 7 de diciembre de 2010, asuntos acumulados C-585/08 y C-144/09. Accesible en: http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0585&lang1=es&type=NOT&ancre. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS (TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA): Sentencia de 26 de octubre de 2006, asunto C-168/05. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A62005CJ0168. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS (TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA): Sentencia de 20 de enero de 2005, asunto C-464/01. Accesible en: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=49857&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=550885. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS (TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA): Sentencia de 21 de noviembre de 2002, asunto C-473/00. Accesible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A62000CJ0473. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS (TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA): Sentencia de 22 de noviembre de 2001, asuntos acumulados C-541/99 y C-542-99. Accesible en:

http://curia.europa.eu/juris/liste.jsf?num=C-541/99. Último acceso: 08.08.2018.

TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS (TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA): Sentencia de 03 de julio de 1997, asunto C-269/95. Accesible en: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=43682&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=550885. Último acceso: 08.08.2018

TRIBUNAL SUPREMO: Sentencia 1385/2017, del 05 de abril de 2017. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7992000&links=uso%20mixto&optimize=20170419&publicinterface=true. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 1923/2015, del 30 de abril de 2015. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7385947&links=1258&optimize=20150521&publicinterface=true. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 4050/2010, del 15 de julio de 2010. Accesible en: http://www.poderjudicial.es/search/documento/TS/5698482/proteccion%20de%20datos%20de%20caracter%20personal/20100812. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 3491/2009, de 25 de mayo de 2009. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=4616972&links=abusiva&optimize=20090625&publicinterface=true. Último acceso: 08.08.2008.

TRIBUNAL SUPREMO: Sentencia 1105/2003, de 27 de noviembre de 2003. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2806722&links=%221105%2F2003%22&optimize=20040124&publicinterface=true. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 1280/2002, de 31 de diciembre de 2002. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=3243497&links=%221280%2F2002%22&optimize=20030703&publicinterface=true. Último acceso: 08.08.2018

TRIBUNAL SUPREMO: Sentencia 1137/1998, de 20 de febrero de 1999. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2339589&links=sumisi%C3%B3n%20expresa&optimize=20040521&publicinterface=true. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 4793/1997, de 5 de julio de 1997. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=3238960&links=&optimize=20030704&publicinterface=true. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 6826/1996, de 30 de noviembre de 1996. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2942125&links=&optimize=20031203&publicinterface=true. Último acceso: 08.08.2018.

TRIBUNAL SUPREMO: Sentencia 5677/1993, de 23 de julio de 1993. Accesible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=2216465&links=&optimize=20040624&publicinterface=true. Último acceso: 08.08.2018.